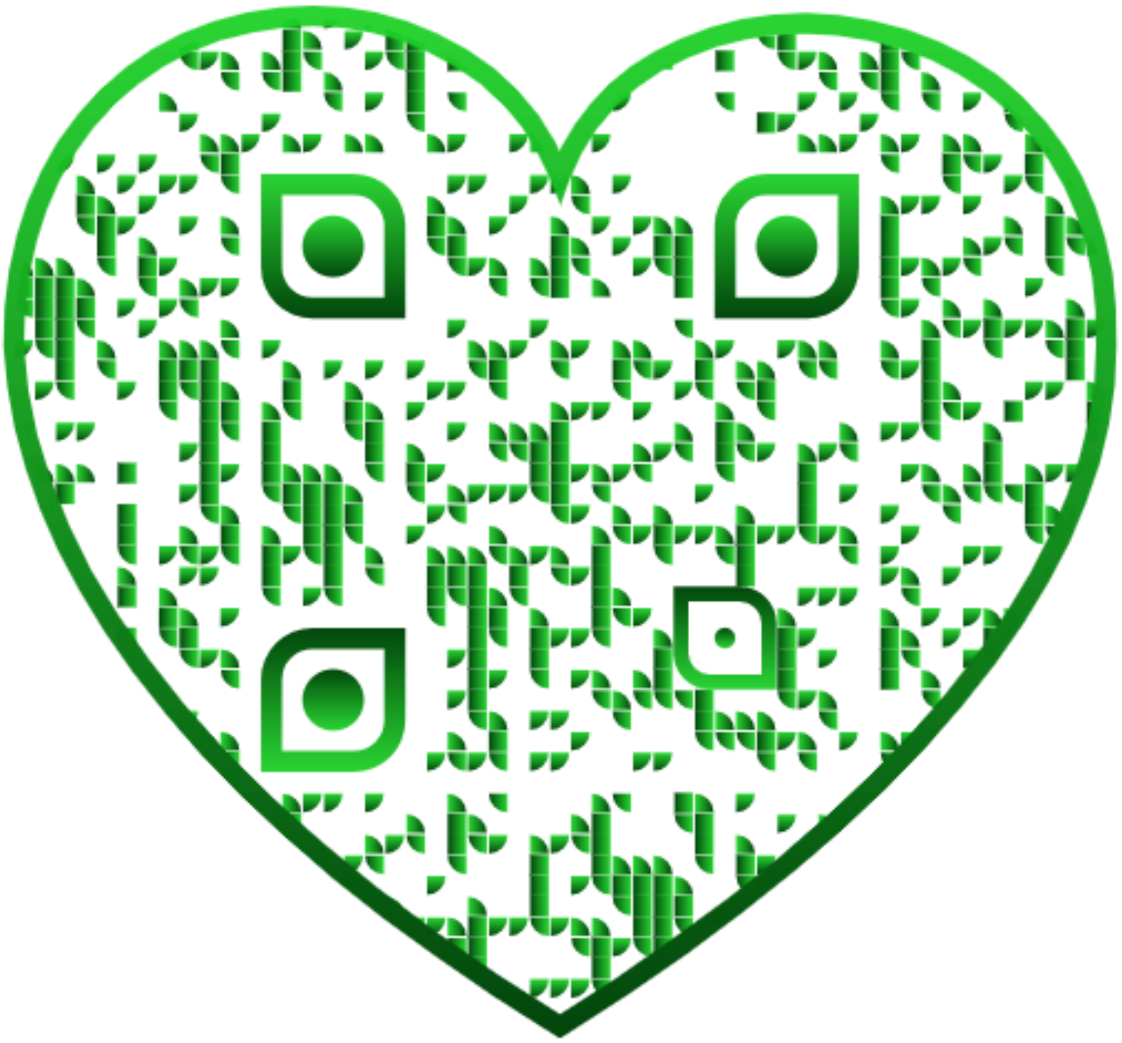
RÉSEAUX ET TÉLÉCOMS



Consultez nos catalogues
sur le Web
http://www.dunod.com
SCIENCES ET TECHNIQUES
INFORMATIQUE Dunod & Microsoft Press
GESTION & MANAGEMENT
SCIENCES HUMAINES
Acheter en ligne
Nouveautés
DUNOD
Microsoft Press
EdiScience ETSF
InterÉditions
Compléments en ligne
Magazine et interviews d'auteurs

RÉSEAUX ET TÉLÉCOMS

Cours et exercices corrigés

Claude Servin
Chargé de cours au CNAM de Paris
et en écoles d'ingénieur
Ancien responsable télécom
au ministère de la Défense

Préface de
Jean-Pierre Arnaud
Professeur au CNAM

DUNOD

Ce pictogramme mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du **photocopillage**.

Le Code de la propriété intellectuelle du 1er juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.

Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation du Centre français d'exploitation du droit de copie (**CFC**, 20 rue des Grands-Augustins, 75006 Paris).

Nouveau tirage corrigé
© Dunod, Paris, 2003
ISBN 2 10 007986 7

Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite selon le Code de la propriété intellectuelle (Art L 122-4) et constitue une contrefaçon réprimée par le Code pénal. • Seules sont autorisées (Art L 122-5) les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective, ainsi que les analyses et courtes citations justifiées par le caractère critique, pédagogique ou d'information de l'œuvre à laquelle elles sont incorporées, sous réserve, toutefois, du respect des dispositions des articles L 122-10 à L 122-12 du même Code, relatives à la reproduction par reprographie.

Préface

Le domaine des Télécommunications et des Réseaux est en pleine effervescence, chaque semaine qui s'écoule apporte sa moisson de nouvelles offres, d'annonces et de propositions de norme. Confronté à ce flux incessant de nouveautés, le praticien doit faire des choix qui s'avéreront stratégiques pour l'entreprise et structurants pour l'avenir de son système d'information. C'est dire l'importance de disposer de bases solides, seules aptes à évaluer sainement la pertinence des solutions proposées par les constructeurs de matériels et les éditeurs de logiciels. Encore faut-il s'entendre sur la constitution de cette base : il ne s'agit pas d'amasser des connaissances plus ou moins vagues ou plus ou moins utiles, mais de construire un socle sur lequel pourra s'appuyer une réflexion personnelle.

Dans la conjoncture actuelle, il n'est guère de tâche plus utile que de transmettre ces connaissances et d'enseigner les méthodes qui permettent d'en tirer profit. L'évolution technologique imposait une nouvelle édition des ouvrages de Claude Servin. Pour distinguer ce qui, dans cette multitude d'évolutions, est suffisamment assuré pour mériter d'être enseigné, il fallait la pratique du terrain d'un homme de réseaux. Il fallait aussi allier à cette expérience de l'ingénieur qui crée des projets celle de l'enseignant qui transmet les savoirs nécessaires à cette création.

Claude Servin possède assurément l'une et l'autre et c'est ce qui donne à son ouvrage un intérêt tout particulier. Ses lecteurs apprécieront une présentation simple des concepts les plus fondamentaux, débarrassés de tout hermétisme et orientés vers l'action et l'ingénierie, sans céder aux modes passagères ou aux complexités inutiles qui encombrent bien des manuels.

Ce sont ces qualités qui lui ont permis de s'inscrire avec réussite dans les enseignements dispensés au Conservatoire National des Arts et Métiers (CNAM) et de jouer le rôle de pivot vers des enseignements plus spécialisés.

Déjà inséré dans le monde du travail, le public du CNAM est exigeant, il vient y chercher une mise en perspective et une rigueur sans faille. Il ne saurait se satisfaire de l'autorité d'un enseignant qui ne pourrait faire preuve de sa capacité à maîtriser les enjeux technologiques actuels. Claude Servin a su les convaincre et, comme les auditeurs qui se pressent nombreux à ses cours et y trouvent l'impulsion pour un approfondissement ultérieur, je suis certain que

le lecteur trouvera à la lecture de cet ouvrage un intérêt soutenu et qu'il sera son compagnon pendant encore de longues années. Les manuels d'enseignement auxquels on continue de se référer une fois entré dans la vie active ne sont pas si nombreux : ayant personnellement l'expérience de la direction de sociétés dans le domaine des réseaux, je ne saurais faire à cet ouvrage un meilleur compliment que de dire qu'il fait partie de ceux-là.

Jean-Pierre ARNAUD
Professeur au Conservatoire National des Arts et Métiers
Titulaire de la chaire de Réseaux

Table des matières

PRÉFACE DE JEAN-PIERRE ARNAUD V

AVANT-PROPOS XXV

CHAPITRE 1 • **HISTORIQUE ET NORMALISATION** 1
1.1 Objet des télécommunications 1
1.2 Bref historique 3
1.3 La normalisation 4
1.4 Principes d'élaboration d'une norme (ISO) 5
1.5 Normes et agrément 5

CHAPITRE 2 • **L'INFORMATION ET SA REPRÉSENTATION DANS LES SYSTÈMES DE TRANSMISSION** 7
2.1 Généralités 7
2.1.1 Les flux d'information 7
2.1.2 Caractéristiques des réseaux de transmission 8
2.2 Représentation de l'information 9
2.2.1 Les différents types d'information 9
2.2.2 Codage des informations 10
2.2.3 Numérisation des informations 15
2.3 La compression de données 20
2.3.1 Généralités 20
2.3.2 Quantification de la compression 20
2.3.3 La compression sans perte 20
2.3.4 Les codages à réduction de bande 21

2.4 Notion de qualité de service 24
2.4.1 Données et contraintes de transmission 24
2.4.2 Les classes de service 25
2.4.3 Conclusion 26

EXERCICES 27

CHAPITRE 3 • **ÉLÉMENTS DE BASE DE LA TRANSMISSION DE DONNÉES** 29
3.1 Classification en fonction du mode de contrôle de l'échange 29
3.1.1 Selon l'organisation des échanges 29
3.1.2 Selon le mode de liaison 30
3.1.3 Les modes de contrôle de la liaison 31
3.2 Classification en fonction des paramètres physiques 32
3.2.1 Transmission parallèle, transmission série 32
3.2.2 Transmission asynchrone, transmission synchrone 34
3.2.3 Selon le mode de transmission électrique 40
3.3 Principe d'une liaison de données 41

EXERCICES 43

CHAPITRE 4 • **LES SUPPORTS DE TRANSMISSION** 45
4.1 Caractéristiques des supports de transmission 46
4.1.1 Bande passante et système de transmission 46
4.1.2 Impédance caractéristique 49
4.1.3 Coefficient de vélocité 51
4.2 Les supports guidés 51
4.2.1 La paire torsadée 51
4.2.2 Le câble coaxial 54
4.2.3 La fibre optique 55
4.2.4 Les liaisons hertziennes 59
4.3 Conclusion 63

EXERCICES 64

CHAPITRE 5 • **LES TECHNIQUES DE TRANSMISSION** 67
5.1 Généralités 67
5.2 La transmission en bande de base 68
5.2.1 Définitions 68
5.2.2 Fonctions d'un codeur/décodeur en bande de base 69
5.2.3 Les principaux codes utilisés 69
5.2.4 Le codeur bande de base ou émetteur récepteur en bande de base 73
5.2.5 Limitations de la transmission en bande de base 74

5.3 La transmission en large bande 78
5.3.1 Principe 78
5.3.2 Les liaisons full duplex 83
5.3.3 Dispositifs complémentaires 84
5.3.4 Exemples de modem 87
5.3.5 Principaux avis du CCITT 89
5.4 La jonction DTE/DCE ou interface 90
5.4.1 Nécessité de définir une interface standard 90
5.4.2 Les principales interfaces 91
5.5 Conclusion 99

EXERCICES 100

CHAPITRE 6 • **NOTIONS DE PROTOCOLES** 103
6.1 La délimitation des données 104
6.1.1 Notion de fanion 104
6.1.2 Notion de transparence 104
6.2 Le contrôle d'intégrité 105
6.2.1 Notion d'erreur 105
6.2.2 Détection d'erreur par clé calculée 107
6.2.3 Les codes autocorrecteurs 113
6.3 Le contrôle de l'échange 114
6.3.1 Du mode Send and Wait aux protocoles à anticipation 114
6.3.2 Le contrôle de flux 123
6.4 La signalisation 126
6.4.1 Définition 126
6.4.2 La signalisation dans la bande 127
6.4.3 La signalisation hors bande 127
6.5 Étude succincte d'un protocole de transmission (HDLC) 129
6.5.1 Généralités 129
6.5.2 Structure de la trame HDLC 130
6.5.3 Les différentes fonctions de la trame HDLC 130
6.5.4 Fonctionnement d'HDLC 133
6.5.5 Les différentes versions du protocole HDLC 137
6.5.6 HDLC et les environnements multiprotocoles 137
6.6 Conclusion 138

EXERCICES 139

© Dunod – La photocopie non autorisée est un délit

CHAPITRE 7 • **LA MUTUALISATION DES RESSOURCES** 141
7.1 La quantification de trafic 141
7.1.1 Généralités 141
7.1.2 Intensité de trafic et taux d'activité 142
7.2 Les concentrateurs 144
7.2.1 Principe 144
7.2.2 Fonctionnalités complémentaires, exemple d'application 145
7.3 Les multiplexeurs 146
7.3.1 Principe 146
7.3.2 Le multiplexage spatial 147
7.3.3 Le multiplexage temporel 149
7.3.4 Comparaison multiplexeur/concentrateur 153
7.4 Conclusion 154

EXERCICES 155

CHAPITRE 8 • **LE CONCEPT DE RÉSEAU** 157
8.1 généralités 157
8.1.1 Définitions 157
8.1.2 Classification des réseaux 158
8.1.3 Topologies physiques des réseaux 159
8.2 Les réseaux à commutation 162
8.2.1 Introduction à la commutation 162
8.2.2 La commutation de circuits 163
8.2.3 La commutation de messages 164
8.2.4 La commutation de paquets 165
8.2.5 Les mécanismes mis en œuvre dans le réseau 171
8.3 Notion d'adressage 172
8.3.1 Définitions 172
8.3.2 L'adressage physique 172
8.4 Notions de nommage 176
8.4.1 Le nommage 176
8.4.2 Notion d'annuaire 177
8.5 L'acheminement dans le réseau 177
8.5.1 Définitions 177
8.5.2 Les protocoles de routage 178
8.6 Adaptation de la taille des unités de données 187
8.6.1 Notion de MTU 187
8.6.2 Segmentation et réassemblage 187

8.7 La congestion dans les réseaux 188
8.7.1 Définition 188
8.7.2 Les mécanismes de prévention de la congestion 189
8.7.3 Résolution ou guérison de la congestion 191
8.8 La voix sur les réseaux en mode paquets 191
8.8.1 Intérêt et contraintes 191
8.8.2 Principe de la paquetisation de la voix 192
8.9 Conclusion 193

EXERCICES 194

CHAPITRE 9 • **LES ARCHITECTURES PROTOCOLAIRES** 195
9.1 Concepts de base 196
9.1.1 Principe de fonctionnement d'une architecture en couches 196
9.1.2 Terminologie 197
9.2 Organisation du modèle de référence 200
9.2.1 Concepts ayant conduit à la modélisation 200
9.2.2 Description du modèle de référence 202
9.3 Étude succincte des couches 207
9.3.1 La couche physique 207
9.3.2 La couche liaison de données 208
9.3.3 La couche réseau 208
9.3.4 La couche transport 212
9.3.5 La couche session 217
9.3.6 La couche présentation 218
9.3.7 La couche application 220
9.3.8 Devenir du modèle OSI 223
9.4 Les architectures constructeurs 225
9.4.1 Architecture physique d'un système de téléinformatique 225
9.4.2 Origine des architectures constructeurs 225
9.4.3 SNA (System Network Architecture) d'IBM 226
9.4.4 DSA (Distributed System Architecture) de BULL 229
9.5 Conclusion 230

EXERCICES 231

CHAPITRE 10 • **L'ARCHITECTURE TCP/IP** 233
10.1 Généralités 233
10.1.1 Origine 233
10.1.2 Principe architectural 234

© Dunod – La photocopie non autorisée est un délit

10.1.3 Description générale de la pile et applications TCP/IP 235
10.1.4 Les mécanismes de base de TCP/IP 236
10.1.5 Les instances de normalisation 238
10.2 L'adressage du réseau logique 239
10.2.1 Principe de l'adressage IP 239
10.2.2 Les techniques d'adressage dans le réseau IP 241
10.3 Le routage dans le réseau IP 250
10.3.1 L'adressage d'interface 250
10.3.2 Concept d'interface non numérotée 251
10.4 Le protocole IP et les utilitaires réseaux 251
10.4.1 Généralités 251
10.4.2 Structure du datagramme IP 252
10.4.3 Contrôle de la fragmentation sous IP 255
10.4.4 Le protocole ICMP 256
10.4.5 L'utilitaire PING 257
10.4.6 La résolution d'adresses 258
10.4.7 Les utilitaires de configuration 261
10.4.8 Conclusion 262
10.5 Transmission Control Protocol (TCP) 263
10.5.1 Généralités 263
10.5.2 Le message TCP et les mécanismes associés 263
10.6 Les protocoles de liaison (point à point) 272
10.6.1 Généralités 272
10.6.2 SLIP, Serial Line Internet Protocol (RFC 1055) 272
10.6.3 PPP, Point to Point Protocol (RFC 1548) 273
10.7 Exemples d'applications TCP/IP 275
10.7.1 Le service de noms (DNS) 275
10.7.2 Le transfert de fichiers 278
10.7.3 L'émulation de terminal (TELNET) 281
10.8 D'IPv4 à IPv6 283
10.8.1 Les lacunes d'IPv4 283
10.8.2 Le datagramme IPv6 284
10.8.3 L'adressage dans IPv6 287
10.9 Conclusion 291

EXERCICES 292

CHAPITRE 11 • **LES RÉSEAUX DE TRANSPORT X.25, FRAME RELAY, ATM ET BOUCLE LOCALE** 295
11.1 Le plan de transmission 295
11.1.1 Généralités 295
11.1.2 La synchronisation des réseaux 297
11.1.3 La hiérarchie plésiochrone (PDH) 300
11.1.4 La hiérarchie synchrone (SDH) 302
11.2 Le plan de service 306
11.2.1 Généralités 306
11.2.2 Le protocole X.25 307
11.2.3 Évolution vers les hauts débits 323
11.2.4 Le Frame Relay 324
11.2.5 L'ATM (Asynchronous Transfer Mode) 335
11.2.6 Les réseaux d'opérateurs 355
11.3 L'accès aux réseaux, la boucle locale 356
11.3.1 Définition 356
11.3.2 Organisation de la distribution des accès 356
11.3.3 La Boucle Locale Radio (BLR) 358
11.3.4 Les accès hauts débits 358
11.4 Conclusion 361

EXERCICES 362

CHAPITRE 12 • **LES RÉSEAUX LOCAUX ETHERNET, CSMA/CD, TOKEN RING, VLAN...** 367
12.1 Introduction 367
12.1.1 Définition 367
12.1.2 Distinction entre réseau local et informatique traditionnelle 368
12.1.3 Réseaux locaux et accès aux systèmes traditionnels 368
12.1.4 Constituants d'un réseau local 369
12.1.5 Les réseaux locaux et la normalisation 371
12.2 Étude succincte des différentes couches 372
12.2.1 La couche physique 372
12.2.2 La sous-couche MAC 377
12.2.3 La couche liaison (LLC) 381
12.3 Les réseaux CSMA/CD, IEEE 802.3/Ethernet 385
12.3.1 Les origines d'Ethernet 385
12.3.2 Principe du CSMA/CD 385
12.3.3 Caractéristiques communes aux réseaux Ethernet/802.3 387
12.3.4 Trame Ethernet/IEEE 802.3 389
12.3.5 Les différentes versions d'Ethernet 390

© Dunod – La photocopie non autorisée est un délit

12.4 L'anneau à jeton, IEEE 802.5 395
12.4.1 Généralités 395
12.4.2 Principe général du jeton sur anneau 396
12.4.3 Comparaison Ethernet/Token Ring 401
12.5 Le jeton adressé ou Token bus, IEEE 802.4 403
12.5.1 Généralités 403
12.5.2 Fonctionnement du jeton sur bus 404
12.5.3 Format des données 406
12.6 Le réseau 100 VG Any Lan, 802.12 407
12.6.1 Généralités 407
12.6.2 Le DPAM 407
12.7 La commutation dans les LAN 409
12.7.1 Principe de base 409
12.7.2 Notion d'architecture des commutateurs 410
12.7.3 Les différentes techniques de commutation 412
12.7.4 Les différents modes de commutation 412
12.7.5 Ethernet Full Duplex 413
12.8 Les réseaux virtuels ou VLAN 413
12.8.1 Principes généraux des VLAN 413
12.8.2 Les différents niveaux de VLAN 414
12.8.3 L'identification des VLAN (802.1Q) 415
12.9 Les réseaux sans fil 417
12.9.1 Généralités 417
12.9.2 Architecture générale des réseaux sans fil 418
12.9.3 Les réseaux 802.11 419
12.10 Aspect protocolaire 421
12.10.1 Généralités 421
12.10.2 Les piles ISO 421
12.10.3 La pile IPX/SPX 422
12.10.4 La pile NETBIOS 424
12.11 Les canaux hauts débits 426
12.11.1 HiPPI 426
12.11.2 Fibre Channel Standard 427
12.12 Conclusion 428

EXERCICES 429

CHAPITRE 13 • **LES RÉSEAUX MÉTROPOLITAINS FDDI, DQDB, ATM...** 431
13.1 FDDI (Fiber Distributed Data Interface) 431
13.1.1 Généralités 431
13.1.2 La méthode d'accès : le jeton temporisé 433
13.1.3 Architecture du réseau FDDI 435
13.1.4 Aspects physiques 436
13.1.5 Format des trames FDDI 438
13.1.6 Fonctionnement général de l'anneau 439
13.1.7 Évolution de FDDI : FDDI-II 439
13.1.8 Conclusion 440
13.2 DQDB (Distributed Queue Dual Bus) 440
13.2.1 Généralités 440
13.2.2 Architecture générale de DQDB 442
13.2.3 Algorithme d'accès au support 443
13.2.4 Format de l'unité de donnée DQDB 445
13.2.5 Le service SMDS et CBDS 446
13.3 Les réseaux locaux ATM 447
13.3.1 Généralités 447
13.3.2 « Classical IP » ou « IP over ATM » 449
13.3.3 LAN Emulation 451
13.3.4 Interconnexion de réseaux LANE (MPOA) 458
13.4 Conclusion 460
EXERCICES 461
CHAPITRE 14 • **INTERCONNEXION DES RÉSEAUX** 463
14.1 Généralités 463
14.1.1 Définition 463
14.1.2 Problématique de l'interconnexion 463
14.1.3 Notions de conversion de service et de protocole 464
14.1.4 L'encapsulation ou *tunneling* 465
14.1.5 Les différents types de relais 465
14.2 Les répéteurs 466
14.3 Les ponts 467
14.3.1 Généralités 467
14.3.2 Les différents types de ponts 468
14.3.3 Les ponts transparents 469
14.3.4 Le Spanning Tree Protocol (STP) ou arbre recouvrant 471
14.3.5 Ponts à routage par la source 474
14.3.6 Le pontage par translation 477

© Dunod – La photocopie non autorisée est un délit

14.4 Les routeurs 477
14.4.1 Généralités 477
14.4.2 Les techniques de routage 480
14.4.3 Routage et qualité de service 494
14.4.4 Routage multicast 498
14.4.5 Fonctions annexes des routeurs 502
14.5 Les passerelles applicatives 506

EXERCICES 507

CHAPITRE 15 • **LA TÉLÉPHONIE** 511
15.1 Principes généraux de la téléphonie 511
15.2 Organisation du réseau téléphonique 512
15.2.1 Architecture traditionnelle 512
15.2.2 Gestion du réseau 513
15.3 Établissement d'une communication téléphonique 514
15.3.1 Principe d'un poste téléphonique 514
15.3.2 Principe du raccordement d'usager 515
15.3.3 La mise en relation Usager/Usager 515
15.3.4 La numérotation 517
15.3.5 Les modes de signalisation 518
15.4 Évolution de la téléphonie, le RNIS 520
15.4.1 De l'accès analogique à l'accès numérique 520
15.4.2 Le concept d'intégration de services 520
15.4.3 Structure du réseau 521
15.4.4 Le raccordement d'usager 522
15.4.5 Les services du RNIS 524
15.4.6 Signalisation et le réseau RNIS 527
15.5 La téléphonie et la mobilité 537
15.5.1 Principes généraux 537
15.5.2 Gestion de l'abonné et du terminal 539
15.5.3 L'interface radio 540
15.5.4 Description succincte des différents systèmes en service 543
15.5.5 Le service transport de données sur la téléphonie mobile 543
15.5.6 La mobilité et l'accès à Internet 545
15.5.7 Évolution des systèmes de téléphonie mobile, l'UMTS 546
15.5.8 La téléphonie satellitaire 546
15.6 Conclusion 547

EXERCICES 548

CHAPITRE 16 • **INSTALLATION D'ABONNÉ ET RÉSEAU PRIVÉ DE TÉLÉPHONIE** 549
16.1 Les autocommutateurs privés 549
16.1.1 Généralités 549
16.1.2 Architecture d'un PABX 550
16.1.3 Les téléservices et applications vocales offerts par les PABX 550
16.1.4 PABX et transmission de données 556
16.2 L'installation d'abonné 557
16.2.1 Généralités 557
16.2.2 Dimensionnement du raccordement au réseau de l'opérateur 558
16.3 Les réseaux privés de PABX 560
16.3.1 Principes généraux 560
16.3.2 La signalisation et type de liens 562
16.4 Principes des réseaux voix/données 570
16.4.1 Généralités 570
16.4.2 Les réseaux de multiplexeurs 570
16.4.3 La voix paquetisée 571
16.5 La voix sur ATM 578
16.6 La voix et le Frame Relay 579
16.7 La voix et téléphonie sur IP 581
16.7.1 Généralités 581
16.7.2 TCP/IP et le temps réel 582
16.7.3 L'architecture H.323 de l'UIT 585
16.7.4 Le protocole SIP de l'IETF (RFC 2543) 588
16.7.5 Le protocole MGCP 591
16.8 Conclusion 591

EXERCICES 592

CHAPITRE 17 • **LA SÉCURITÉ DES SYSTÈMES D'INFORMATION** 595
17.1 Généralités 595
17.2 La sûreté de fonctionnement 595
17.2.1 Principes généraux de la sûreté 595
17.2.2 Les systèmes à tolérance de panne 595
17.2.3 La sûreté environnementale 597
17.2.4 Quantification 599
17.3 La sécurité 601
17.3.1 Généralités 601
17.3.2 La protection des données 601
17.3.3 La protection du réseau 611

© Dunod – La photocopie non autorisée est un délit

17.4 Le commerce électronique 620
17.4.1 Le paiement off-line (ecash) 620
17.4.2 Le paiement on-line 620
17.5 Conclusion 621
EXERCICES 622
CHAPITRE 18 • **ADMINISTRATION DES RÉSEAUX** 625
18.1 Généralités 625
18.1.1 Définition 625
18.1.2 Principe général 625
18.1.3 Structure d'un système d'administration 626
18.2 L'administration vue par l'ISO 626
18.2.1 Généralités 626
18.2.2 Les différents modèles 627
18.3 L'administration dans l'environnement TCP/IP 630
18.3.1 Principes généraux 630
18.3.2 Les MIB 631
18.3.3 Le protocole SNMP 634
18.4 SNMP et ISO 635
18.5 Les plates-formes d'administration 635
18.5.1 Les outils d'administration des couches basses 636
18.5.2 Les hyperviseurs 636
18.5.3 Les systèmes intégrés au système d'exploitation 636
18.6 Conclusion 636
EXERCICES 637
CHAPITRE 19 • **INTRODUCTION À L'INGÉNIERIE DES RÉSEAUX** 639
19.1 Généralités 639
19.2 Services et tarification 640
19.3 Eléments d'architecture des réseaux 640
19.3.1 Structure de base des réseaux 640
19.3.2 Conception du réseau de desserte 641
19.3.3 Conception du réseau dorsal 643
19.4 Dimensionnement et évaluation des performances 644
19.4.1 Généralités 644
19.4.2 Les réseaux en mode circuit 645
19.4.3 Les réseaux en mode paquets 647
19.5 Conclusion 652
EXERCICES 653

CHAPITRE 20 • **SOLUTIONS DES EXERCICES** 657

ANNEXES 745

A. Définitions 746

B. Abaques d'Erlang 747

C. Liste des abréviations et sigles utilisés 749

BIBLIOGRAPHIE 757

GLOSSAIRE 759

INDEX 801

© Dunod – La photocopie non autorisée est un délit

Liste des exercices

Exercice 2.1 Code ASCII, Algorithme de changement de casse
Exercice 2.2 Codage de Huffman
Exercice 2.3 Télécopieur
Exercice 2.4 Numérisation du son
Exercice 2.5 Numérisation et débit binaire
Exercice 2.6 Rapport signal à bruit et loi de quantification A
Exercice 2.7 Image RVB

Exercice 3.1 Organisation des échanges
Exercice 3.2 Transmission parallèle
Exercice 3.3 Transmission synchrone et asynchrone
Exercice 3.4 Éléments d'accès au réseau
Exercice 3.5 Transmission asynchrone
Exercice 3.6 Temps de transfert d'information

Exercice 4.1 Notion de décibel
Exercice 4.2 Portée d'une liaison hertzienne
Exercice 4.3 Bande passante d'une fibre optique

Exercice 5.1 Caractéristiques d'un modem
Exercice 5.2 Débit possible sur un canal TV
Exercice 5.3 Rapport Signal/Bruit
Exercice 5.4 Le Null Modem
Exercice 5.5 Contrôle de flux matériel

Exercice 5.6 Modem dissymétrique
Exercice 5.7 Rapidité de modulation

Exercice 6.1 Calcul de CRC
Exercice 6.2 Probabilité de recevoir un message erroné
Exercice 6.3 Taux de transfert
Exercice 6.4 Échange HDLC version LAP-B

Exercice 7.1 Intensité de trafic et taux d'activité
Exercice 7.2 Application numérique E et θ
Exercice 7.3 Trame MIC
Exercice 7.4 Multiplexeur

Exercice 8.1 Évaluation du nombre de liaisons
Exercice 8.2 Table de routage
Exercice 8.3 Temps de transfert sur un réseau

Exercice 9.1 Fonctions et couches OSI
Exercice 9.2 Adresse SAP d'une émission FM
Exercice 9.3 Encapsulation
Exercice 9.4 Mode connecté et mode non connecté
Exercice 9.5 Terminal virtuel
Exercice 9.6 Contrôle de flux et transferts isochrones
Exercice 9.7 Contrôle de flux et classe de transport 0
Exercice 9.8 Référencement d'une connexion de transport
Exercice 9.9 Connexion de transport et connexion de session
Exercice 9.10 Les types de variables d'ASN-1

Exercice 10.1 Masque de sous-réseau
Exercice 10.2 Masque de sous-réseau et dysfonctionnement (figure 20.26)
Exercice 10.3 Table ARP
Exercice 10.4 Trace TCP/IP

Exercice 11.1 SDH/PDH
Exercice 11.2 Reconstitution d'un paquet d'appel
Exercice 11.3 Dialogue X.25
Exercice 11.4 Définition d'un protocole
Exercice 11.5 Protocole ATM
Exercice 11.6 Priorité ou réservation de ressources

© Dunod – La photocopie non autorisée est un délit

Exercice 11.7 Encapsulation de données
Exercice 11.8 Évolution de l'encapsulation d'IP

Exercice 12.1 Distinction entre CSMA/CD IEEE 802.3 et Ethernet.
Exercice 12.2 Adressage MAC
Exercice 12.3 Notation canonique et non canonique
Exercice 12.4 Comparaison des topologies et des méthodes d'accès
Exercice 12.5 Séquence de synchronisation bit en 802.3 et 802.5
Exercice 12.6 Rapidité de modulation
Exercice 12.7 Longueur virtuelle de l'anneau 802.5
Exercice 12.8 Conception d'un réseau Ethernet à 100 Mbit/s
Exercice 12.9 Efficacité du protocole 802.5 à 100 Mbit/s
Exercice 12.10 Temps de rotation du jeton
Exercice 12.11 Commutateur ou hub ?
Exercice 12.12 Plan d'adressage d'une entreprise

Exercice 13.1 FDDI et Token Ring
Exercice 13.2 Données de la classe Isochrone
Exercice 13.3 L'acquittement dans FDDI
Exercice 13.4 Rotation des données sur le réseau FDDI
Exercice 13.5 État des compteurs dans DQDB

Exercice 14.1 Interconnexion d'un réseau 802.3 et 802.5
Exercice 14.2 Spanning Tree Protocol (STR)
Exercice 14.3 Protocoles RIP/OSPF
Exercice 14.4 Agrégation de routes
Exercice 14.5 Adresses multicast
Exercice 14.6 Comparaison pont/routeur
Exercice 14.7 Masque de sous-réseau
Exercice 14.8 Routage statique

Exercice 15.1 Capacité d'un autocommutateur
Exercice 15.2 Itinérance
Exercice 15.3 Système Iridium
Exercice 15.4 Schéma de réutilisation des fréquences
Exercice 15.5 Protocole D (Q.931)

Exercice 16.1 Utilisation de l'abaque d'Erlang
Exercice 16.2 Trafic sur un faisceau

Exercice 16.3 Raccordement d'un PABX
Exercice 16.4 Trafic d'un centre d'appel
Exercice 16.5 Réseau voix/données
Exercice 16.6 Dimensionnement d'un réseau Frame Relay voix/données
Exercice 16.7 Comparaison H.323 et SIP

Exercice 17.1 MTTR/MTBF
Exercice 17.2 Systèmes à clés symétriques ou secrètes
Exercice 17.3 Algorithme à translation de César
Exercice 17.4 Algorithme de substitution de Vigenère
Exercice 17.5 Algorithme du RSA
Exercice 17.6 Système de Diffie-Hellman

Exercice 18.1 Analyse de la trace
Exercice 18.2 SNMP et charge du réseau

Exercice 19.1 Service de vidéotex
Exercice 19.2 Informatisation d'un magasin
Exercice 19.3 Réalisation d'un réseau privé d'entreprise
Exercice 19.4 Caractéristique mémoire d'un routeur
Exercice 19.5 Temps de transit dans un réseau

© Dunod – La photocopie non autorisée est un délit

Avant-propos

Les réseaux de télécommunication constituent aujourd'hui une formidable passerelle entre les hommes et les cultures, mais transporter des informations aussi différentes que la voix, les données et les images nécessite des techniques de plus en plus élaborées, une bonne connaissance des mécanismes de base et une maîtrise des technologies utilisées. Bien connaître les limites technologies pour être capable de concevoir, de spécifier et d'utiliser correctement les moyens mis à notre disposition constitue l'objectif essentiel de cet ouvrage.

Le début de ce siècle est marqué par une évolution considérable des techniques, or certaines technologies, qui peuvent paraître vieillissantes à certains, sont encore très présentes dans les entreprises. De plus, elles constituent bien souvent le fondement des techniques actuelles et c'est volontairement que l'auteur a maintenu dans cet ouvrage une étude succincte des technologies propriétaires, des réseaux X.25, des réseaux métropolitains et les LAN ATM...

L'étude du modèle OSI a été retenue car, par son formalisme, c'est une référence architecturale à laquelle tous les développements modernes, même s'ils ne sont pas conformes au modèle, se réfèrent. Le protocole TCP/IP est largement développé, notamment par l'introduction de l'étude des mécanismes d'IPv6. Les techniques d'actualité font toutes l'objet d'une étude appropriée, en particulier les réseaux sans fils, la boucle locale et ADSL, MPLS, les VLAN et les VPN. La téléphonie d'entreprise et en particulier l'intégration voix/données font l'objet d'un exposé approfondi conduisant à l'intégration de la voix sur IP. Éléments fondamentaux des réseaux d'entreprise, l'étude de la sécurité et l'administration sont traitées en détail, tandis qu'une initiation à l'ingénierie des réseaux conclut cet ouvrage.

À la fin de chaque chapitre des exercices ou des études de cas corrigés sont proposés. Les corrections sont détaillées afin de permettre à tous de comprendre le cheminement du raisonnement.

REMERCIEMENTS

Il ne conviendrait pas de terminer cet avant-propos sans remercier tous ceux, amis et famille, qui grâce à leur soutien, leurs conseils et de fastidieuses relectures, ont permis que cet ouvrage soit ce qu'il est, et tout particulièrement à Laurence DUCHIEN, professeur à l'université de

Lille pour ses nombreuses remarques et suggestions. Enfin, j'exprime ma reconnaissance à Maxime MAIMAN qui par son premier ouvrage m'a fait découvrir et aimer le monde des réseaux ainsi qu'à Solange GHERNAOUTI-HÉLIE qui m'a témoigné sa confiance en accueillant dans sa collection mes premiers ouvrages *Télécoms 1* et *Télécoms 2* dont le présent ouvrage *Réseaux et Télécoms* est issu.

Chapitre **1**

Historique et normalisation

1.1 OBJET DES TÉLÉCOMMUNICATIONS

Les télécommunications recouvrent toutes les techniques (filaires, radio, optiques, etc.) de transfert d'information quelle qu'en soit la nature (symboles, écrits, images fixes ou animées, son, ou autres). Ce mot, introduit en 1904 par Estaurié (polytechnicien, ingénieur général des télégraphes 1862-1942), fut consacré en 1932 à la conférence de Madrid qui décida de rebaptiser l'Union Télégraphique Internationale en Union Internationale des Télécommunications (**UIT**).

Aujourd'hui, avec la déferlante Internet, les télécommunications ont débordé les domaines de la télégraphie et de la téléphonie. Une ère nouvelle est née, celle de la communication. Cette révolution n'a été rendue possible que par une formidable évolution des technologies. Les progrès réalisés dans le traitement du signal ont autorisé la banalisation des flux de données et la convergence des techniques. Cette convergence, illustrée figure 1.1 implique de la part des professionnels une adaptation permanente. Cette dernière ne sera possible que si l'ingénieur ou le technicien possède une base de connaissance suffisamment vaste, c'est l'objectif de cet ouvrage.

Dans la première étape, illustrée figure 1.1, les flux voix et données sont de nature fonctionnelle et physique différentes. Chaque système dispose de son propre réseau. Notons que la transmission de données sur le réseau téléphonique fut interdite par France Télécom jusqu'en 1960. Lors de la libéralisation de ce service, le débit autorisé était d'abord limité à 1 200 bit/s, puis 2 400 bit/s en 1976 et 4 800 bit/s en 1980.

Dans la seconde étape, la voix fait l'objet d'une numérisation. Les flux physiques sont banalisés et comme tel, peuvent être transportés par un même réseau (réseau de transport). Cependant, les réseaux d'accès restent fonctionnellement différents et les usagers accèdent toujours aux services par des voies distinctes.

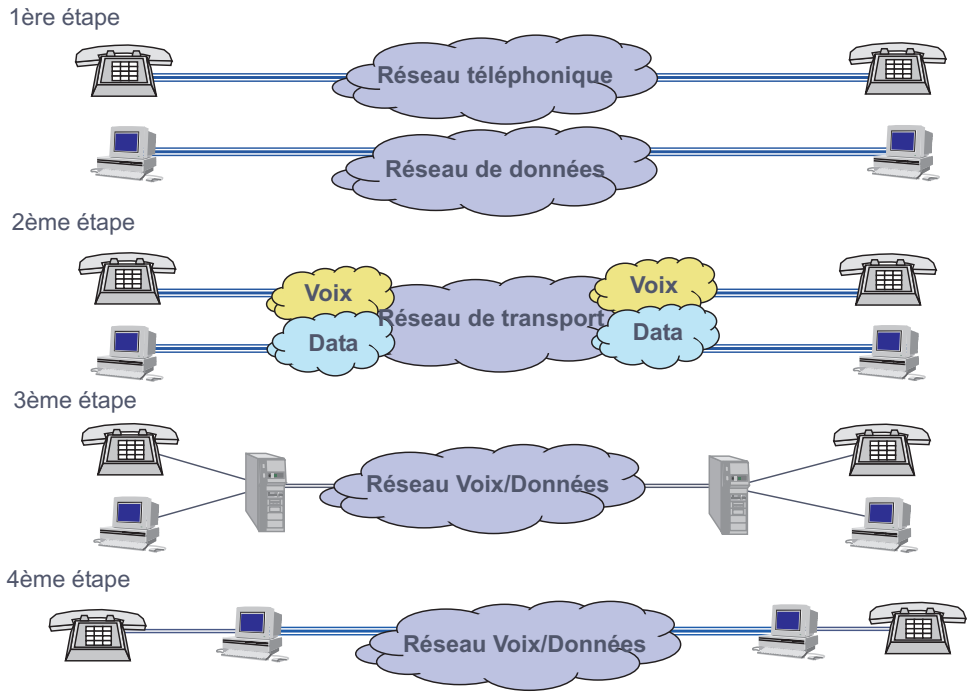


Figure 1.1 Schématisation de l'évolution des télécommunications.

La troisième étape poursuit la banalisation des flux. La voix n'est plus seulement numérisée, les différents éléments d'informations sont rassemblés en paquets, comme la donnée. On parle alors de « voix paquétisée », permettant ainsi un traitement de bout en bout identique pour les deux flux. Dans cette approche, le protocole de transport est identique, mais les protocoles usagers restent différents. L'usager n'a plus besoin que d'un seul accès physique au réseau de transport (réseau voix/données). Les flux sont séparés par un équipement (équipement voix/données) localisé chez l'usager et sont traités par des systèmes différents.

La quatrième étape consiste en une intégration complète, les équipements terminaux ont une interface d'accès identique mais des fonctionnalités applicatives différentes. La voix et la donnée peuvent, non seulement cohabiter sur un même réseau, mais collaborer dans les applications informatiques finales : c'est le couplage informatique téléphonie de manière native. Dans cette approche les protocoles utilisés dans le réseau de transport et ceux utilisés dans le réseau de l'usager sont identiques pour les deux types de flux.

Cependant, quelle que soit la complexité du système, le principe reste toujours le même : il faut assurer un transfert fiable d'information d'une entité communicante A vers une entité communicante B.

Figure 1.2 Constituants de base d'un système de transmission de données.

Ce qui nécessite (figure 1.2) :

– des données traduites dans une forme compréhensible par les calculateurs,
– un lien entre les entités communicantes, que ce lien soit un simple support ou un réseau de transport,
– la définition d'un mode d'échange des données,
– la réalisation d'un système d'adaptation entre les calculateurs et le support,
– un protocole[1] d'échange.

Ces différents points seront traités dans les chapitres qui suivent. Cependant, on ne saurait entreprendre l'étude d'une technique sans disposer, pour celle-ci, de quelques repères historiques sur son évolution. Finalement, les télécommunications n'auraient pas connu un tel essor si des organismes particuliers, les organismes de normalisation, n'avaient permis, grâce à leurs travaux, l'interopérabilité des systèmes.

1.2 BREF HISTORIQUE

On peut estimer que l'histoire des télécommunications commence en 1832, date à laquelle le physicien américain Morse (1791-1872) eut l'idée d'un système de transmission codée (alphabet Morse). Les premiers essais, en 1837, furent suivis d'un dépôt de brevet en 1840. La première liaison officielle fut réalisée en 1844. C'est en 1856 que la France adopta le système Morse. La première liaison transocéanique, réalisée en 1858, ne fonctionna qu'un mois (défaut d'isolement du câble immergé).

Parallèlement, la phonie (le téléphone) se développait. Les principes formulés par le français Charles Bourseul conduisirent à un dépôt de brevet, pour un système téléphonique, par Graham Bell (1847-1922) et Eliska Gray (1835-1901). Les demandes furent déposées à deux heures d'intervalle.

Marconi (1874-1937) réalisa en 1899 une première liaison télégraphique par onde hertzienne entre la France et l'Angleterre. Mais, c'est Lee de Forest (1873-1961) qui avec l'invention de la triode ouvrit véritablement la voie aux transmissions longues distances. La première liaison téléphonique transocéanique par ondes hertziennes fut réalisée en 1927.

Le principe de la numérisation du signal (MIC, Modulation par Impulsions Codées) fut décrit en 1938 par Alei Reever, mais il fallut attendre les progrès de l'électronique pour réaliser les premiers codeurs. L'évolution s'accéléra, en 1948, avec l'invention du transistor (Bardeen, Brattain, Shockley des laboratoires Bell) qui par sa faible consommation et son échauffement limité, ouvrit des voies nouvelles. C'est ainsi que le premier câble téléphonique transocéanique fut posé en 1956 avec 15 répéteurs immergés.

Enfin, en 1962, le satellite Telstar 1 autorise la première liaison de télévision transocéanique, tandis que 7 ans plus tard, on peut vivre en direct les premiers pas de l'Homme sur la Lune.

1. *Protocole* : convention définissant un ensemble de règles à suivre pour effectuer un échange d'informations.
Procédure : séquence de règles à suivre pour accomplir un processus.
Pour le *télécommunicant* ces deux termes sont synonymes, cependant il semble préférable d'utiliser le terme procédure lorsque les règles sont simples et de réserver le terme protocole à un ensemble de règles plus complexes.

© Dunod – La photocopie non autorisée est un délit

L'évolution des techniques conduit à la création de réseaux pour offrir des services de transport d'information ou des téléservices au public. En 1978 la première liaison numérique (Transfix) est effectuée et 1979 voit l'ouverture au public du premier réseau mondial de transmission de données par paquets X.25 (France : Transpac).

L'explosion de la télématique se concrétise avec l'expérience de Vélizy (1981), le Minitel envahit les foyers domestiques. Les télécommunications sont aujourd'hui, de manière tout à fait transparente, utilisées journellement par tous : télécopie, Minitel, cartes de crédit et surtout Internet...

1.3 LA NORMALISATION

La normalisation peut être vue comme un ensemble de règles destinées à satisfaire un besoin de manière similaire. La normalisation dans un domaine technique assure une réduction des coûts d'étude, la rationalisation de la fabrication et garantit un marché plus vaste. Pour le consommateur, la normalisation est une garantie d'interfonctionnement, d'indépendance vis-à-vis d'un fournisseur et de pérennité des investissements.

En matière de télécommunication, la normalisation est issue d'organismes divers. Du groupement de constructeurs aux organismes internationaux, la normalisation couvre tous les domaines de la communication. D'une manière générale, la normalisation ne s'impose pas, sauf celle émanant de **l'ETSI** (*European Telecommunications Standard Institute*) qui normalise les réseaux publics et leurs moyens d'accès.

Les principaux groupements de constructeurs sont :

– **ECMA** (*European Computer Manufactures Association*), à l'origine constituée uniquement de constructeurs européens (Bull, Philips, Siemens...) l'ECMA comprend aujourd'hui tous les grands constructeurs mondiaux (DEC, IBM, NEC, Unisys...). En matière de télécommunications, l'ECMA comprend deux comités : le TC23 pour l'interconnexion des systèmes ouverts et le TC24 pour les protocoles de communication ;

– **EIA** (*Electronic Industries Association*) connue, essentiellement, pour les recommandations RS232C, 449 et 442.

Les principaux organismes nationaux auxquels participent des industriels, administrations et utilisateurs sont :

– **AFNOR**, Association Française de NORmalisation,

– **ANSI**, *American National Standard Institute* (USA),

– **DIN**, *Deutsches Institut für Normung* (Allemagne), bien connu pour sa normalisation des connecteurs (prises DIN) ;

– **BSI**, *British Standard Institute* (Grande Bretagne).

Les organismes internationaux :

– **ISO**, *International Standardization Organization*, regroupe environ 90 pays. L'ISO est organisée en Technical Committee (TC) environ 200, divisés en Sub-Committee (SC) eux-mêmes subdivisés en Working Group (WG) ; la France y est représentée par l'AFNOR ;

– **CEI**, Commission Électrotechnique Internationale, affiliée à l'ISO en est la branche électricité ;

– **UIT-T**, Union Internationale des Télécommunications secteur des télécommunications, qui a succédé en 1996 au CCITT (Comité Consultatif International Télégraphie et Téléphonie), publie des recommandations. Celles-ci sont éditées tous les 4 ans sous forme de recueils. Les domaines d'application sont identifiés par une lettre :
  – V, concerne les modems et les interfaces,
  – T, s'applique aux applications télématiques,
  – X, désigne les réseaux de transmission de données,
  – I, se rapporte au RNIS,
  – Q, intéresse la téléphonie et la signalisation.

L'IEEE, *Institute of Electrical and Electronics Enginers*, société savante constituée d'industriels et d'universitaires, est essentiellement connue par ses spécifications sur les bus d'instrumentation (IEEE 488) et par ses publications concernant les réseaux locaux (IEEE 802), reprises par l'ISO (IS 8802).

Le panorama serait incomplet si on omettait de citer **l'IAB**, *Internet Architecture Board*, qui a la charge de définir la politique à long terme d'Internet, tandis que **l'IETF** (*Internet Engineering Task Force*) assure par ses publications (**RFC** *Request For Comments*) l'homogénéité de la communauté TCP/IP et Internet.

1.4 PRINCIPES D'ÉLABORATION D'UNE NORME (ISO)

La rédaction d'une norme est une succession de publications, la durée entre le projet et la publication définitive peut être très longue. En effet, chaque partie tente d'y défendre ses intérêts économiques et commerciaux. D'une manière générale, un projet de normalisation est formalisé dans un document brouillon qui expose les concepts en cours de développement (*Draft*) ; lorsque ce document arrive à une forme stable, les « drafts » sont publiés (*Draft proposable*), chaque pays émet son avis (vote). Enfin, une forme quasi définitive est publiée, elle constitue une base de travail pour les constructeurs (*Draft International Standard*). La norme appelée *International Standard* (**IS**) est ensuite publiée.

1.5 NORMES ET AGRÉMENT

Généralement, ce n'est pas parce qu'un équipement répond à une norme que celui-ci est autorisé, de fait, à se raccorder à un réseau public. En effet, l'opérateur public se doit de garantir aux usagers de son réseau une certaine qualité de service. Il lui appartient de vérifier qu'un nouvel équipement ne perturbe ni le fonctionnement du réseau sur lequel il est raccordé, ni d'autres services télématiques.

Cette mesure, souvent perçue comme une mesure protectionniste, est en vigueur dans tous les pays. En France, c'est la Direction Générale des Postes et Télécommunications (ex-Direction de la Réglementation Générale ou DRG) qui est l'organe d'homologation des matériels de télécommunication.

© Dunod – La photocopie non autorisée est un délit

Chapitre **2**

L'information et sa représentation dans les systèmes de transmission

2.1 GÉNÉRALITÉS

2.1.1 Les flux d'information

L'acheminement, dans un même réseau, d'informations aussi différentes que les données informatiques, la voix ou la vidéo implique que chacune de ces catégories d'information ait une représentation identique vis-à-vis du système de transmission et que le réseau puisse prendre en compte les contraintes spécifiques à chaque type de flux d'information (figure 2.1).

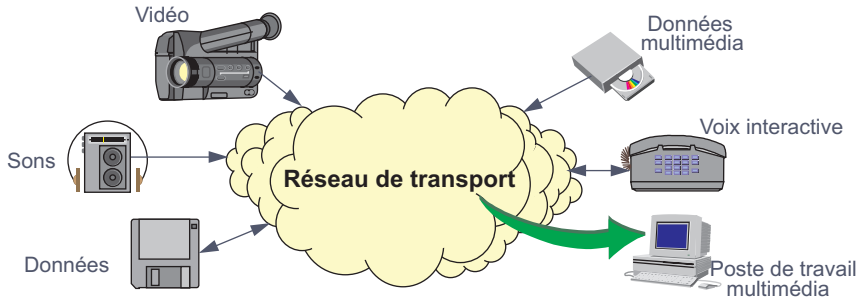


Figure 2.1 Le réseau et les différents flux d'information.

Afin de qualifier ces différents flux vis-à-vis du système de transmission, nous définirons succinctement les caractéristiques essentielles d'un réseau de transmission[1]. Nous examinerons ensuite le mode de représentation des informations. Enfin, nous appliquerons les résultats

1. Ces différentes notions seront revues et appronfondies dans la suite de cet ouvrage.

aux données, à la voix et à l'image pour en déduire les contraintes de transfert spécifiques à chaque type de flux.

2.1.2 Caractéristiques des réseaux de transmission

Notion de débit binaire

Les systèmes de traitement de l'information emploient une logique à deux états ou binaire. L'information traitée par ceux-ci doit être traduite en symboles compréhensibles et manipulables par ces systèmes. L'opération qui consiste à transformer les données en éléments binaires s'appelle le **codage** ou **numérisation** selon le type d'information à transformer.

On appelle débit binaire (D) le nombre d'éléments binaires, ou nombre de bits, émis sur le support de transmission pendant une unité de temps. C'est l'une des caractéristiques essentielles d'un système de transmission. Le débit binaire s'exprime par la relation :

$$D = \frac{V}{t}$$

avec D (débit) en bits par seconde (bit/s[2]), V le volume à transmettre exprimé en bits et t la durée de la transmission en seconde.

Le débit binaire mesure le nombre d'éléments binaires transitant sur le canal de transmission pendant l'unité de temps (figure 2.2).

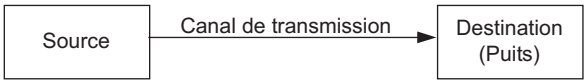


Figure 2.2 Schématisation d'un système de transmission.

Notion de rapport signal sur bruit

Les signaux transmis sur un canal peuvent être perturbés par des phénomènes électriques ou électromagnétiques désignés sous le terme générique de **bruit**. Le bruit est un phénomène qui dénature le signal et introduit des erreurs.

Le rapport entre la puissance du signal transmis et celle du signal de bruit qualifie le canal vis-à-vis du bruit. Ce rapport, appelé rapport signal sur bruit (S/N avec N pour *Noise*), s'exprime en dB (décibel[3]) :

$$S/N_{dB} = 10 \log_{10} S/N_{(\text{en puissance})}$$

Notion de taux d'erreur

Les phénomènes parasites (bruit) perturbent le canal de transmission et peuvent affecter les informations en modifiant un ou plusieurs bits du message transmis, introduisant ainsi des

2. L'unité officielle de débit est le bit/s (invariable). L'abréviation bps pouvant être confondue avec byte par seconde ne sera pas utilisée dans cet ouvrage. Rappelons que le terme bit provient de la contraction des termes « binary digit ».

3. Le décibel ou dB (10^{e} du bel) est une unité logarithmique sans dimension. Elle exprime le rapport entre deux grandeurs de même nature. Le rapport Signal/Bruit peut aussi s'exprimer par le rapport des tensions, la valeur est alors $S/N_{\text{dB}} = 20 \log_{10} S/N_{(\text{en tension})}$.

erreurs dans le message. On appelle **taux d'erreur binaire** (Te ou **BER**, *Bit Error Rate*) le rapport du nombre de bits reçus en erreur au nombre de bits total transmis.

$$Te = \frac{\text{Nombre de bits en erreur}}{\text{Nombre de bits transmis}}$$

Notion de temps de transfert

Le temps de transfert, appelé aussi temps de transit ou temps de latence, mesure le temps entre l'émission d'un bit, à l'entrée du réseau et sa réception en sortie du réseau. Ce temps prend en compte le temps de propagation sur le ou les supports et le temps de traitement par les éléments actifs du réseau (nœuds). Le temps de transfert est un paramètre important à prendre en compte lorsque la source et la destination ont des échanges interactifs.

Pour un réseau donné, le temps de transfert n'est généralement pas une constante, il varie en fonction de la charge du réseau. Cette variation est appelée gigue ou *jitter*.

Notion de spectre du signal

Le mathématicien français Joseph Fourier (1768-1830) a montré que tout signal périodique de forme quelconque pouvait être décomposé en une somme de signaux élémentaires sinusoïdaux (fondamental et harmoniques) autour d'une valeur moyenne (composante continue) qui pouvait être nulle. L'ensemble de ces composantes forme le spectre du signal ou bande de fréquence occupée par le signal (largeur de bande).

2.2 REPRÉSENTATION DE L'INFORMATION

2.2.1 Les différents types d'information

Les informations transmises peuvent être réparties en deux grandes catégories selon ce qu'elles représentent et les transformations qu'elles subissent pour être traitées dans les systèmes informatiques. On distingue :

– Les données discrètes, l'information correspond à l'assemblage d'une suite d'éléments indépendants les uns des autres (suite discontinue de valeurs) et dénombrables (ensemble fini). Par exemple, un texte est une association de mots eux-mêmes composés de lettres (symboles élémentaires).

– Les données continues ou analogiques (figure 2.3) résultent de la variation continue d'un phénomène physique : température, voix, image... Un capteur fournit une tension électrique proportionnelle à l'amplitude du phénomène physique analysé : signal analogique (signal qui varie de manière analogue au phénomène physique). Un signal analogique peut prendre une infinité de valeurs dans un intervalle déterminé (bornes).

Pour traiter ces informations par des équipements informatiques il est nécessaire de substituer à chaque élément d'information une valeur binaire représentative de l'amplitude de celui-ci. Cette opération porte le nom de codage de l'information (codage à la source) pour les informations discrètes et numérisation de l'information pour les informations analogiques.

© Dunod – La photocopie non autorisée est un délit

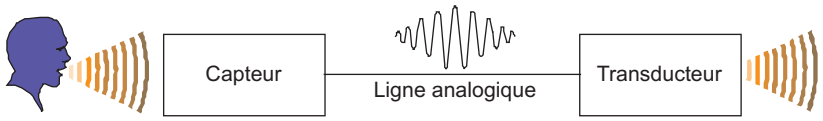


Figure 2.3 Le signal analogique.

2.2.2 Codage des informations

Définition

Coder l'information consiste à faire correspondre (bijection) à chaque symbole d'un alphabet (élément à coder) une représentation binaire (mot code). L'ensemble des mots codes constitue le code (figure 2.4). Ces informations peuvent aussi bien être un ensemble de commandes d'une machine outil que des caractères alphanumériques... C'est à ces derniers codes que nous nous intéresserons. Un code alphanumérique peut contenir :

- Des chiffres de la numérotation usuelle [0..9] ;
- Des lettres de l'alphabet [a..z, A..Z] ;
- Des symboles nationaux [é, è,...] ;
- Des symboles de ponctuation [, ; : . ? ! ...] ;
- Des symboles semi-graphiques [▉ ╟ ╢] ;
- Des commandes nécessaires au système [Saut de ligne, Saut de page, etc.].

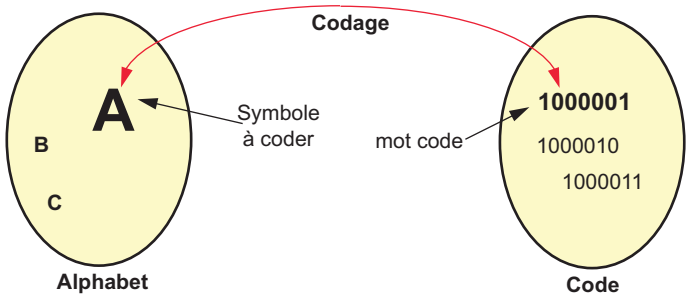


Figure 2.4 Principe du codage des données.

Les différents types de code

Le codage des différents états d'un système peut s'envisager selon deux approches. La première, la plus simple, considère que chacun des états du système est équiprobable. La seconde prend en compte la fréquence d'apparition d'un état. Cette approche conduit à définir deux types de code : les codes de longueur fixe et les codes de longueur variable.

➤ Les codes de longueur fixe

Chaque état du système est codé par un certain nombre de bits, appelé longueur du code, longueur du mot code ou encore code à n moments.

– Avec 1 bit on peut coder 2 états (0,1)
– Avec 2 bits on peut coder 4 états (00, 01, 10, 11)
– Avec 3 bits on peut coder 8 états (000, 001, 010, 011, 100, 101, 110, 111)
D'une manière générale :
– Avec n bits on code 2^n états

Le nombre d'états pouvant être codés par un code de n bits s'appelle puissance lexicographique du code que l'on note :

$$P = 2^n$$

En généralisant, le nombre de bits nécessaires pour coder P états est n, tel que :

$$2^{(n-1)} < P \leqslant 2^n$$

Le nombre de bits pour coder P symboles est donc[4]

$$n = \log_2 P$$

Ce nombre de bits (n) représente la quantité d'information (Q) apportée par la connaissance d'un état du système. Lorsque dans un système, tous les états sont équiprobables, la quantité d'information apportée par la connaissance d'un état est la même quel que soit l'état connu. Si l'information est représentée par deux valeurs équiprobables (0 ou 1, pile ou face...), la quantité d'information, exprimée en shannon[5] ou plus simplement en bit, est :

$$Q = \log_2 2 = 1 \text{ shannon ou } 1 \text{ bit.}$$

Le bit est la quantité d'information qui correspond au lever de doute entre deux symboles équiprobables.

Lorsque tous les états ne sont pas équiprobables, la quantité d'information est d'autant plus grande que la probabilité de réalisation de l'état est faible. Si p est la probabilité de réalisation de l'état P, la quantité d'information apportée par la connaissance de P est :

$$Q = \log_2 1/p$$

Application : combien de bits sont nécessaires pour coder toutes les lettres de l'alphabet et quelle est la quantité d'information transmise par une lettre (en supposant équiprobable l'apparition de chaque lettre) ?

Le nombre de bits nécessaires, pour coder P valeurs, est donné par la relation :

$$2^{(n-1)} < P \leqslant 2^n \quad \text{si} \quad P = 26 \quad \text{on a} \quad 2^4 < 26 \leqslant 2^5$$

soit 5 bits pour coder les 26 éléments.

4. Le logarithme d'un nombre est la valeur par laquelle il faut élever la base pour retrouver ce nombre (n = base $^{\log N}$). Le logarithme de 8 à base 2 est 3 car $2^3 = 8$

5. Les premiers travaux sur la théorie de l'information sont dus à Nyquist (1924). La théorie de l'information fut développée par Shannon en 1949. Les principes établis à cette époque régissent toujours les systèmes de transmission de l'information.

© Dunod – La photocopie non autorisée est un délit

La quantité d'information, exprimée en shannon ou plus simplement en bits, est donnée par la relation :

$$Q = \log_2(1/p)$$

où p représente la probabilité d'apparition d'un symbole. Ici, p = 1/26

$$Q = \log_2(26) = 3,32 \log_{10}(26) = 3,32 \cdot 1,4149 = 4,66 \text{ shannon ou bits}$$

La quantité d'information calculée ici correspond à la valeur optimale de la longueur du code dans un système de symboles équiprobables. Les codes usuels utilisent 5 éléments (Code Baudot), 7 éléments (Code ASCII appelé aussi CCITT N° 5 ou encore IA5) ou 8 éléments (EBCDIC).

Le code Baudot, code télégraphique à 5 moments ou alphabet international N° 2 ou CCITT N° 2, est utilisé dans le réseau Télex. Le code Baudot autorise 2^5 soit 32 caractères, ce qui est insuffisant pour représenter toutes les lettres de l'alphabet (26), les chiffres (10) et les commandes (Fin de ligne...). Deux caractères particuliers permettent la sélection de deux pages de codes soit au total une potentialité de représentation de 60 caractères.

Le code **ASCII** (figure 2.5), *American Standard Code for Information Interchange***,** dont la première version date de 1963, est le code générique des télécommunications. Code à 7 moments, il autorise 128 caractères (2^7). Les 32 premiers symboles correspondent à des commandes utilisées dans certains protocoles de transmission pour en contrôler l'exécution. La norme de base prévoit des adaptations aux particularités nationales (adaptation à la langue). Ce code, étendu à 8 moments, constitue l'alphabet de base des micro-ordinateurs de type PC. Le code **EBCDIC,** *Extended Binary Coded Decimal Interchange Code*, code à 8 moments, d'origine IBM est utilisé dans les ordinateurs du constructeur. Le code EBCDIC a, aussi, été adopté par d'autres constructeurs pour leurs calculateurs tels que BULL.

Caractères nationaux

Jeu de commandes

BITS				b_7	0	0	0	0	1	1	1	1
				b_6	0	0	1	1	0	0	1	1
				b_5	0	1	0	1	0	1	0	1
b_4	b_3	b_2	b_1		0	1	2	3	4	5	6	7
0	0	0	0	0	NUL	DLE	SP	0	à	P		p
0	0	0	1	1	SOH	DC1	!	1	A	Q	a	q
0	0	1	0	2	STX	DC2	"	2	B	R	b	r
0	0	1	1	3	ETX	DC3	£	3	C	S	c	s
0	1	0	0	4	EOT	DC4	$	4	D	T	d	t
0	1	0	1	5	ENQ	NAK	%	5	E	U	e	u
0	1	1	0	6	ACK	SYN	'	6	F	V	f	v
0	1	1	1	7	BEL	ETB	(	7	G	W	g	w
1	0	0	0	8	BS	CAN	)	8	H	X	h	x
1	0	0	1	9	HT	EM	.	9	I	Y	i	y
1	0	1	0	A	LF	SUB		:	J	Z	j	z
1	0	1	1	B	VT	ESC	,	;	K		k	é
1	1	0	0	C	FF	ES		<	L	ç	l	ù
1	1	0	1	D	CR	GS		¨	M	§	m	è
1	1	1	0	E	SO	RS		>	N	^	n	¨
1	1	1	1	F	SI	US	/	?	O	–	o	DEL

Signification des caractères de commande

Symbole	Signification	
ACK	Acknowledge	Accusé de réception
BEL	Bell	Sonnerie
BS	Backspace	Retour arrière
CAN	Cancel	Annulation
CR	Carriage Return	Retour chariot
DC	Device control	Commande d'appareil auxiliaire
DEL	Delete	Oblitération
DLE	Data Link Escape	Caractère d'échappement
EM	End Medium	Fin de support
ENQ	Enquiry	Demande
EOT	End Of Transmission	Fin de communication
ESC	Escape	Echappement
ETB	End of Transmission Block	Fin de bloc de transmission
ETX	End Of Text	Fin de texte
FE	Format Effector	Commande de mise en page
FF	Form Feed	Présentation de formule
FS	File Separator	Séparateur de fichiers
GS	Group Separator	Séparateur de groupes
HT	Horizontal Tabulation	Tabulation horizontale
LF	Line Feed	Interligne
NAK	Negative Acknowledge	Accusé de réception négatif
NUL	Null	Nul
RS	Record Separator	Séparateur d'articles
SI	Shift IN	En code
SO	Shift Out	Hors code
SOH	Start Of Heading	Début d'en-tête
SP	Space	Espace
STX	Start Of Text	Début d'en-tête
SYN	Synchronous idle	Synchronisation
TC	Transmission Control	Commande de transmission
US	Unit Separator	Séparateur de sous-article
VT	Vertical Tabulation	Tabulation verticale

Figure 2.5 Le code ASCII.

➤ Les codes de longueur variable

Lorsque les états du système ne sont pas équiprobables, la quantité d'information apportée par la connaissance d'un état est d'autant plus grande que cet état a une faible probabilité de se réaliser. La quantité moyenne d'information apportée par la connaissance d'un état, appelée **entropie**, est donnée par la relation :

$$H = \sum_{i=1}^{i=n} p_i \log_2 \frac{1}{p_i}$$

où p_i représente la probabilité d'apparition du symbole de rang i.

L'entropie représente la longueur optimale du codage des symboles du système. Déterminons la longueur optimale du code (entropie) pour le système décrit par le tableau ci-dessous. À des fins de simplicité, chaque état est identifié par une lettre.

© Dunod – La photocopie non autorisée est un délit

État	Probabilité
E	0,48
A	0,21
S	0.12
T	0.08
U	0.06
Y	0.05

La longueur optimale du mot code :

$$H = -(0{,}48 \log_2 0{,}48 + 0{,}21 \log_2 0{,}21 + 0{,}12 \log_2 0{,}12 + 0{,}08 \log_2 0{,}08 + 0{,}06 \log_2 0{,}06 + 0{,}05 \log_2 0{,}05)$$

$$H = -3{,}32[(0{,}48 \log_{10} 0{,}48 + 0{,}21 \log_{10} 0{,}21 + 0{,}12 \log_{10} 0{,}12 + 0{,}08 \log_{10} 0{,}08 + 0{,}06 \log_{10} 0{,}06 + 0{,}05 \log_{10} 0{,}05)]$$

$$H = 1,92$$

Le code optimal utile est de 1,92 bit, alors que l'utilisation d'un code à longueur fixe nécessite 3 bits pour coder les 6 états de ce système ($2^2 < 6 \leqslant 2^3$).

Il n'existe pas de code qui permette d'atteindre cette limite théorique. Cependant, Huffman introduit en 1952 une méthode de codage qui prend en compte la fréquence d'occurrence des états et qui se rapproche de cette limite théorique.

Construction du code de Huffman (figure 2.6) :

1. lecture complète du fichier et création de la table des symboles ;
2. classement des symboles par ordre des fréquences décroissantes (occurrence) ;
3. réductions successives en rassemblant en une nouvelle occurrence les deux occurrences de plus petite fréquence ;
4. l'occurrence obtenue est insérée dans la table et celle-ci est à nouveau triée par ordre décroissant ;
5. les réductions se poursuivent jusqu'à ce qu'il n'y ait plus d'élément ;
6. construire l'arbre binaire en reliant chaque occurrence à la racine ;
7. le codage consiste à lire l'arbre du sommet aux feuilles en attribuant par exemple la valeur 0 aux branches basses et 1 aux branches hautes.

La longueur moyenne (Lmoy) du code (figure 2.6) est de :

$$L\text{moy} = 0{,}48 \cdot 1 + 0{,}21 \cdot 2 + 0{,}12 \cdot 3 + 0{,}08 \cdot 4 + 0{,}06 \cdot 5 + 0{,}05 \cdot 5 = 2{,}13$$

Le codage de Huffman permet de réduire le nombre de bits utilisés pour coder l'information. Dépendant du contexte, il impose, avant la transmission, d'établir une convention (Huffman modifié utilisé en télécopie groupe 3) ou de transmettre, avant les données, le contenu de la table construite par l'émetteur.

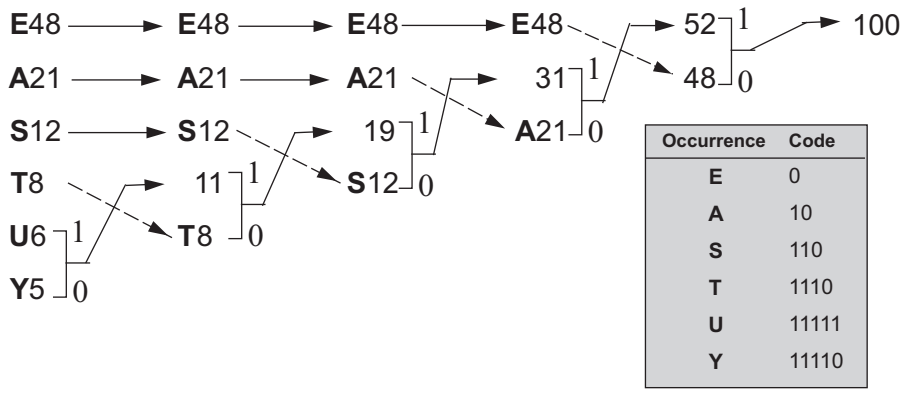


Figure 2.6 Arbre d'Huffman.

D'ASCII à l'Unicode

Le codage ASCII (7 bits) ou ISO-646 ne permet de coder que 127 caractères, il réserve 12 codes pour prendre en compte les particularités nationales. L'internationalisation des communications, notamment avec Internet, a mis au premier plan les problèmes de codage des textes.

Une première extension a été réalisée par la norme ISO-8859-x (8 bits). ISO-8859-x utilise les 128 premiers caractères du code ASCII, le symbole x renvoie vers des tables qui complètent le jeu originel de 96 caractères autorisant ainsi les écritures à base de caractères latins, cyrilliques, arabes, grecs et hébraïques. Le codage ISO-8859-x doit être préféré, sur Internet, à tout autre code chaque fois que cela est possible.

Le décodage d'un texte nécessite qu'il identifie le code utilisé et que le destinataire puisse interpréter ce code, ceci a conduit à définir un code unique sur 16 ou 32 bits permettant la représentation de toutes les langues du monde : l'Unicode (16 bits) qui reprend les spécifications du code ISO 10646 UCS-2 (*Universal Character Set*).

2.2.3 Numérisation des informations

Principe

Numériser une grandeur analogique consiste à transformer la suite continue de valeurs en une suite discrète et finie. À cet effet, on prélève, à des instants significatifs, un échantillon du signal et on exprime son amplitude par rapport à une échelle finie (quantification).

Le récepteur, à partir des valeurs transmises, reconstitue le signal d'origine. Une restitution fidèle du signal nécessite que soient définis :

– l'intervalle d'échantillonnage qui doit être une constante du système (fréquence d'échantillonnage) ;
– l'amplitude de l'échelle de quantification, celle-ci doit être suffisante pour reproduire la dynamique du signal (différence d'amplitude entre la valeur la plus faible et la valeur la plus forte) ;
– que chaque valeur obtenue soit codée.

© Dunod – La photocopie non autorisée est un délit

La figure 2.7 représente les différentes étapes de la numérisation du signal. À intervalle régulier (période d'échantillonnage), on prélève une fraction du signal (échantillon). Puis, on fait correspondre à l'amplitude de chaque échantillon une valeur (quantification), cette valeur est ensuite transformée en valeur binaire (codification).

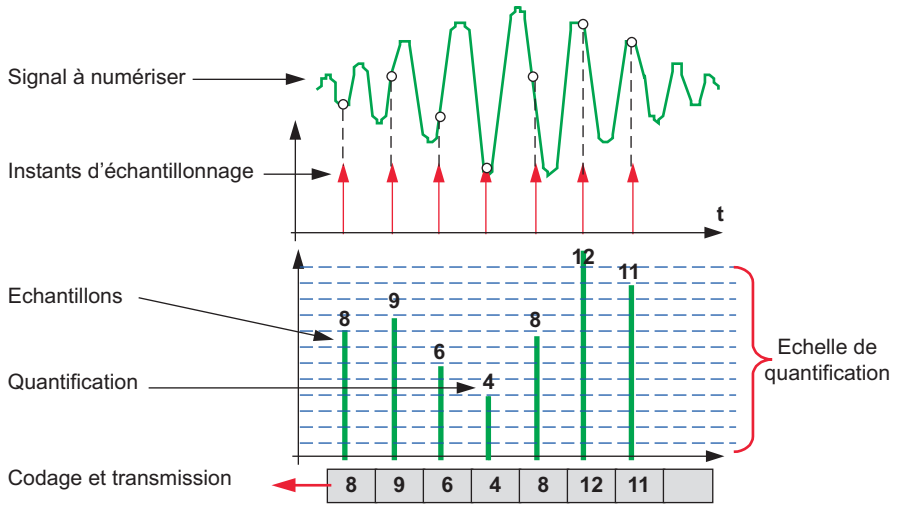


Figure 2.7 Numérisation d'un signal analogique.

La quantification définit des valeurs en escalier (par bond) alors que le phénomène à quantifier varie de façon continue. Aussi, quel que soit le nombre de niveaux utilisés, une approximation est nécessaire, celle-ci introduit une erreur dite de quantification ou bruit de quantification qui est la différence entre la valeur réelle de l'échantillon et la valeur quantifiée.

Pour reproduire correctement le signal à l'arrivée, le récepteur doit disposer d'un minimum d'échantillons. Il existe donc une relation étroite entre la fréquence maximale des variations du signal à discrétiser et le nombre d'échantillons à prélever.

Soit un signal dont le spectre est limité et dont la borne supérieure vaut F_{max}, Shannon a montré que si F_e est la fréquence d'échantillonnage, le spectre du signal échantillonné est le double de F_{max} et est centré autour de F_e, $2F_e$... nF_e. Par conséquent, pour éviter tout recouvrement de spectre, le signal à échantillonner doit être borné (filtre) à une fréquence supérieure telle que F_{max} soit inférieure à la moitié de l'intervalle d'écartement des spectres (Fe). La figure 2.8 illustre cette relation appelée **relation de Shannon**.

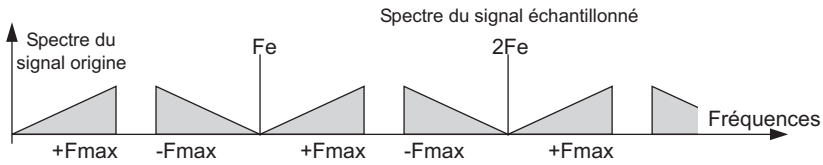


Figure 2.8 Spectre d'échantillonnage.

On en déduit que la fréquence minimale d'échantillonnage (fréquence de Nyquist) d'un signal doit être le double de la fréquence maximale du signal à échantillonner :

$$F_{\text{échantillon}} \geqslant 2 \cdot F_{\text{max du signal}}$$

Figure 2.9 Structure élémentaire d'un convertisseur analogique/numérique.

Application à la voix

Un canal téléphonique utilise une plage de fréquence ou Bande Passante (**BP**) allant de 300 Hz à 3 400 Hz. Si on prend 4 000 Hz comme fréquence maximale à reproduire, la fréquence d'échantillonnage minimale est de :

$$F_e \geqslant 2 \cdot F_{\max} = 2 \cdot 4\,000 = 8\,000 \text{ Hz}$$

Soit 8 000 échantillons par seconde, ce qui correspond, pour chaque échantillon à une durée de 125 µs (1/8 000). Pour une restitution correcte (dynamique[6] et rapport signal à bruit), la voix devrait être quantifiée sur 12 bits (4 096 niveaux). Les contraintes de transmission en rapport avec le débit conduisent à réduire cette bande. L'utilisation d'une loi quantification logarithmique permet de ramener la représentation numérique de la voix à 8 bits (7 bits pour l'amplitude et un bit de signe), tout en conservant une qualité de reproduction similaire à celle obtenue avec une quantification linéaire sur 12 bits. Cette opération dite de compression est différente en Europe (loi A) et en Amérique du Nord (loi μ). En codant chaque échantillon sur 8 bits, il est nécessaire d'écouler :

$$8\,000 \cdot 8 = 64\,000 \text{ bits par seconde sur le lien}$$

Ce qui correspond à un débit de 64 000 bit/s. Ce choix correspond à celui du **RNIS** (Réseau Numérique à Intégration de Service ou **ISDN**, *Integrated Service Digital Network*) qui utilise des voies à 64 kbit/s.

Le codage de l'image vidéo

La voix est un phénomène vibratoire, l'oreille perçoit des variations de pression successives qu'elle interprète. L'image est interprétée globalement par l'œil alors qu'elle ne peut être transmise et reproduite que séquentiellement. La discrétisation de l'image nécessite 2 étapes : d'abord une transformation espace/temps qui se concrétise par une analyse de celle-ci, ligne par ligne, puis une décomposition de chaque ligne en points, enfin la quantification de la valeur lumineuse du point, valeur qui est ensuite transmise.

Une image colorée peut être analysée selon 3 couleurs dites **primaires** de longueur d'onde (λ) déterminée. Pour reconstituer l'image d'origine, il suffit de superposer les trois images, c'est la synthèse additive. La figure 2.10 représente le principe de la synthèse additive, le dosage de chacune des sources lumineuses permet de reproduire toutes les couleurs.

6. La dynamique exprime le rapport entre les puissances maximale et minimale du signal.

© Dunod – La photocopie non autorisée est un délit

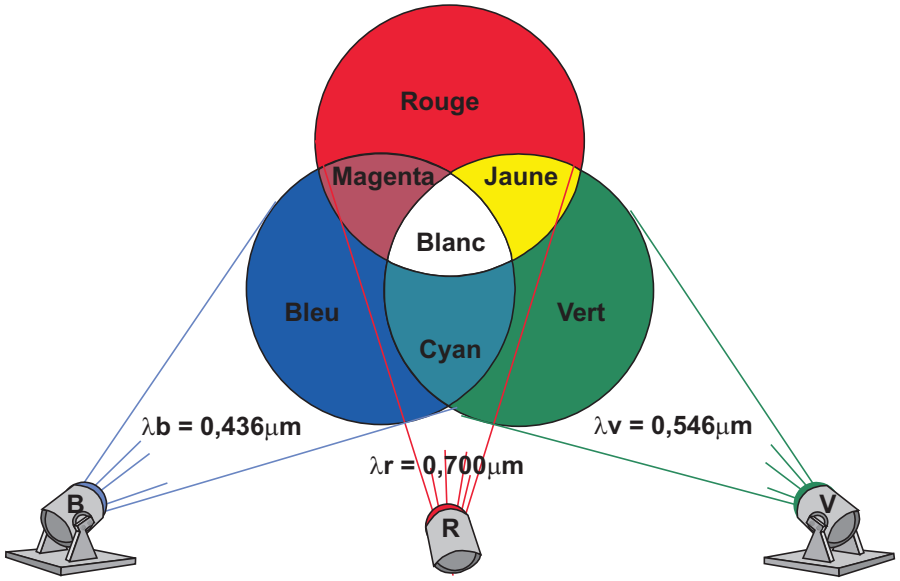


Figure 2.10 La synthèse additive.

Chaque point de l'image est représenté par deux grandeurs, la **luminance** et la **chrominance**. La chrominance, ou information de couleur, est le résultat de la superposition de trois couleurs dites primaires (figure 2.10). Ces deux grandeurs sont reliées entre elles par la relation :

$$Y = 0{,}3\ \mathrm{R} + 0{,}59\ \mathrm{V} + 0{,}11\ \mathrm{B}$$

où : Y est la luminance (échelle des gris),

R l'intensité de la composante de lumière rouge,

V celle de lumière verte,

B celle de lumière bleue.

L'image est dite **RVB** ou **RGB** (*Red*, *Green*, *Blue*), du nom des trois couleurs primaires Rouge, Vert, Bleu. En télévision, pour assurer la compatibilité avec les téléviseurs monochromes, il nous faut transmettre, en plus des informations de chrominance, les informations de luminance (**échelle des gris**).

Les différentes caractéristiques d'une image vidéo constituent un standard. Les paramètres de ces standards sont :

– le format de l'image, à l'origine le même format que le cinéma (4/3), aujourd'hui on évolue vers un format plus large (16/9) ;

– le nombre d'images par seconde déterminé en fonction de la fréquence du réseau électrique pour éviter des effets stroboscopiques, en Europe 25 images/seconde[7], aux USA 30 images/seconde ;

7. Pour augmenter la fréquence de rafraîchissement de l'image, sans augmenter la bande passante nécéssaire, l'analyse et la reproduction se font par demi-image. La première demi-image analyse les lignes impaires, la seconde les lignes paires. L'image est donc reproduite à raison de 50 demi-images par seconde.

– le nombre de lignes a été fixé pour qu'à une distance de vision normale deux lignes consécutives ne soient pas distinguées (les deux lignes doivent être vues sous un angle de moins d'une minute) ;
– le nombre de points par ligne défini pour que la définition horizontale soit identique à la définition verticale.

Le standard d'une image de télévision numérique au format européen (625 lignes, 25 Hz) est caractérisé par :

– le nombre de lignes utiles par image fixé à 576 ;
– le nombre de points par ligne défini à 720[8].
– le nombre d'images par seconde déterminé à 25 images (25 Hz).

Seuls sont transmis : la luminance (Y), pour la compatibilité avec les récepteurs monochromes, et les signaux de chrominance B (Bleu) et R (Rouge)[9]. La connaissance de ces trois grandeurs est nécessaire et suffisante pour reconstituer la quatrième : V (Vert). L'œil ne percevant pas la couleur dans les détails, on se satisfait d'une définition moindre pour l'information couleur que pour l'information monochrome (noir et blanc).

Ainsi, on transmet :

– 720 points par ligne pour le signal Y ;
– 360 points pour chacune des couleurs B et R ;

Au total 1 440 points élémentaires par ligne sont analysés. En se contentant d'une quantification sur 255 niveaux (8 bits, soit 16 millions de couleurs), le nombre de bits nécessaires à la reconstitution de l'image (576 lignes) est donc de :

$$N(\text{bits}) = 1\,440 \cdot 8 \cdot 576 = 6\,635\,520 \text{ bits}$$

À raison de 25 images par seconde (50 demi-images), il faut, pour transmettre une image animée, un débit minimal de :

$$D_{\min} = 6\,635\,520 \cdot 25 = 166 \text{ Mbit/s}.$$

Ce débit est actuellement difficilement réalisable sur les supports de transmission courants. Pour effectuer correctement une transmission d'images animées numérisées, on utilise des techniques particulières de quantification et de compression. Un groupe de travail commun à l'ISO et à la CEI (Commission Électrotechnique Internationale), le *Motion Picture Expert Group* (**MPEG**), est chargé de définir les algorithmes normalisés de compression de son et d'images vidéo.

8. À titre de comparaison : le magnétoscope VHS 250 points/ligne, le magnétoscope SVHS 400 points/ligne, le DVD vidéo 500 points/ligne.

9. On ne transmet pas directement les informations de chrominance, mais les signaux dits de différence de couleur Dr = R – Y, Db = B – Y, Dv = V – Y. Dans ces conditions, l'amplitude du signal V étant la plus importante, la valeur Dv est la plus faible, donc la plus sensible aux bruits de transmission. C'est cette analyse qui a conduit au choix de Dr et Db comme signaux à transmettre.

© Dunod – La photocopie non autorisée est un délit

2.3 LA COMPRESSION DE DONNÉES

2.3.1 Généralités

Si on néglige le temps de propagation du message sur le support, le temps de transmission ou temps de transfert d'un message a pour expression :

$$T_t = \text{Longueur du message en bits/débit de la liaison}$$

Pour un même contenu sémantique, ce temps sera d'autant plus faible que la longueur du message sera petite ou que le débit sera élevé. L'augmentation du débit se heurte à des problèmes technologiques et de coûts. Il peut donc être intéressant de réduire la longueur du message sans en altérer le contenu (la sémantique) : c'est la compression de données.

Les techniques de compression se répartissent en deux familles : les algorithmes réversibles ou sans perte et les algorithmes irréversibles dits avec perte. Les premiers restituent à l'identique les données originelles. Ils s'appliquent aux données informatiques. Le taux de compression obtenu est voisin de 2. Les seconds, dits aussi codes à réduction de bande, autorisent des taux de compression pouvant atteindre plusieurs centaines au détriment de la fidélité de restitution. Utilisés pour la voix et l'image, ils s'apparentent plus à des procédés de codage qu'à des techniques de compression.

2.3.2 Quantification de la compression

La compression se quantifie selon trois grandeurs[10] : le quotient de compression, le taux de compression et le gain de compression.

Le quotient de compression (Q) exprime le rapport entre la taille des données non compressées à la taille des données compressées.

$$Q = \frac{\text{Taille avant compression}}{\text{Taille après compression}}$$

Le taux de compression (T) est l'inverse du quotient de compression.

$$T = 1/Q$$

Enfin, le gain de compression, exprime en % la réduction de la taille des données.

$$G = (1 - T) \cdot 100$$

2.3.3 La compression sans perte

Compression d'un ensemble fini de symboles équiprobables

Quand le nombre de symboles appartient à un ensemble fini, par exemple un catalogue de produits, on peut substituer au symbole un code (référence du produit, code d'erreur...). Cette technique appartient à l'organisation des données.

10. En toute rigueur, les grandeurs définies ci-après ne sont valables que pour les algorithmes de compression sans perte. En effet, pour les algorithmes avec perte, il y a réduction d'information et non compression. Cependant, l'usage étend ces quantifications aux deux types de compression.

La compression de symboles non équiprobables

De nombreuses techniques permettent de réduire la taille de données quelconques. Les trois principales sont :

– Le *Run Length Encoding* (**RLE**) qui consiste à remplacer une suite de caractères identiques par le nombre d'occurrences de ce caractère, on obtient des séquences du type : Échappement/Nombre/Caractère, par exemple la séquence @10A peut signifier, 10 A consécutifs. Ce codage, peu efficace, pour le texte est utilisé pour compresser les images et les fichiers binaires, notamment par MacPaint (Apple).

– Le **codage d'Huffman** ou codage d'entropie substitue à un code de longueur fixe un code de longueur variable. Nécessitant une lecture préalable du fichier et l'envoi du dictionnaire de codage, le code de Huffman est peu efficace. Utilisé en télécopie G3, le code de Huffman modifié (HM) associe, à partir d'un dictionnaire préconstitué, un mot binaire à une séquence de points.

– Le codage par substitution remplace une séquence de caractères prédifinies par un code. Le dictionnaire nécessaire au codage et au décodage est construit dynamiquement. Non transmis il est reconstitué en réception. Connu sous le nom de Lempel-Ziv-Welch (**LZW**), il est utilisé dans les utilitaires de compression PKZIP, ARJ et dans les modems (V.42bis).

2.3.4 Les codages à réduction de bande

Le codage de la voix

La numérisation de la voix selon le procédé **MIC** (Modulation par Impulsion et Codage ou **PCM**, *Pulse Code Modulation*) est adoptée dans tous les réseaux téléphoniques. Cependant, une reproduction correcte de la voix nécessite une quantification sur 12 bits (voir section 2.2.3.2). Cette quantification linéaire introduit un rapport signal à bruit d'autant plus défavorable que la valeur du signal est faible. Cette observation et la nécessité de réduire la bande ont conduit à adopter des lois de quantification logarithmique.

Ces lois autorisent un codage sur 8 bits avec un rapport signal à bruit pratiquement équivalent à une quantification linéaire sur 12 bits. La figure 2.11 représente la partie positive de la loi A. La loi A, utilisée en Europe, divise l'espace de quantification en 8 intervalles. Chaque intervalle de quantification (sauf les deux premiers) est le double du précédent. À l'intérieur de chaque intervalle, on opère une quantification linéaire sur 16 niveaux. Ainsi, un échantillon est représenté par 8 bits (figure 2.11) :

– le premier indique la polarité du signal (P),

– les trois suivants identifient le segment de quantification (S),

– enfin, les quatre derniers représentent la valeur dans le segment (V).

En téléphonie mobile et dans les réseaux en mode paquets (voix sur Frame Relay ou sur IP), afin de gagner en bande passante, la voix subit une opération complémentaire de compression. La technique la plus simple, **l'ADPCM**[11] (*Adaptative Differential Pulse Code Modulation*)

11. L'ADPCM64 autorise une bande de 7 kHz pour un débit de 64 kbit/s, il peut être mis en œuvre dans la téléphonie numérique sur RNIS (Réseau Numérique à Intégration de Service).

© Dunod – La photocopie non autorisée est un délit

code, non la valeur absolue de l'échantillon, mais son écart par rapport au précédent. Des techniques plus élaborées prédisent la valeur future à partir des 4 derniers échantillons (**CELP**, *Code Excited Linear Prediction*).

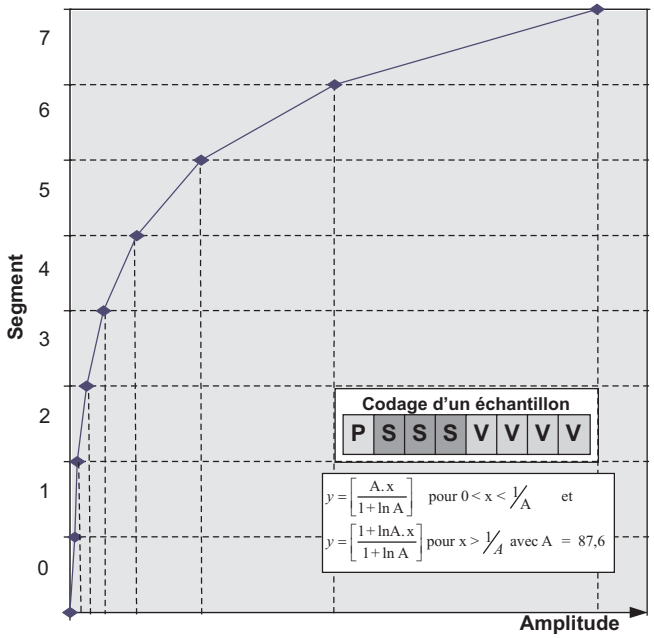


Figure 2.11 La loi de codage A.

La figure 2.12 compare différents algorithmes de compression en fonction du débit qu'ils nécessitent et de la qualité de restitution de la parole. La norme G.711 est utilisée dans la téléphonie fixe traditionnelle. La norme G.729 est mise en œuvre dans la voix sur IP, elle modélise la voix humaine par l'utilisation de filtres.

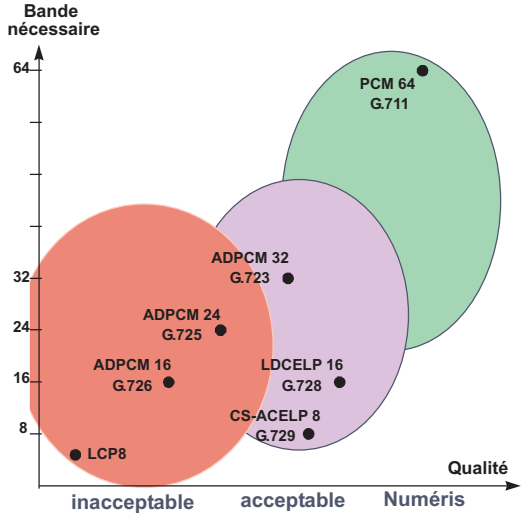


Figure 2.12 Les différents algorithmes de compression du son.

Le codage de l'image

➤ Généralités

La transmission d'images nécessite une largeur de bande importante. Les méthodes de compression efficaces prennent en compte les spécificités de l'information transmise, elles mettent à profit les imperfections de la vision pour réduire la quantité d'information à transmettre. Différentes techniques peuvent être mises en œuvre :

– la quantification scalaire n'attribue pas la même importance à chaque niveau du signal transmis. En recherchant une répartition optimale des niveaux de quantification, on peut réduire la bande nécessaire ;

– la quantification vectorielle est une extension de la méthode précédente, elle opère une quantification sur des blocs (dépendance spatiale entre pixels) ;

– les méthodes prédictives tentent, à partir de la valeur des points voisins, de déterminer la valeur du point courant ;

– les méthodes à compensation de mouvements ne transmettent au temps t que la différence entre l'image actuelle et l'image précédente (t – 1) ;

– la croissance rapide des puissances de calcul des machines modernes laisse prévoir un avenir aux méthodes mathématiques (fractales, ondelettes).

Les normes de compression d'images animées (**MPEG-1** novembre 1992, **MPEG-2** mars 1994, **MPEG-4** fin 1998 – *Moving Picture Expert Group*) procèdent des principes précédents et autorisent des images de qualité **VHS** (MPEG-1) et de qualité TV (720 × 480 à 30 images/seconde pour le système NTSC[12] et 720 × 576 à 25 images/seconde pour le système PAL[13]) pour la norme MPEG-2. MPEG-2 crée un flux binaire dont le débit varie de 10 à 15 Mbit/s selon le contenu des images.

➤ Principe de la compression MPEG

Les informations contenues dans un flux MPEG permettent de reconstituer complètement une séquence vidéo. La figure 2.13 représente la structure fonctionnelle d'un décodeur MPEG. Après décodage et séparation des informations, le décodeur MPEG comporte trois sous-systèmes : le sous-système de traitement des images, le sous-système de traitement du son associé et enfin le sous-système de synchronisation.

Le standard MPEG repose essentiellement sur la prédiction d'images, il spécifie trois types d'images :

– Les images de référence ou *Intra Pictures* (Images I), ces images sont codées indépendamment du contexte, seul intervient leur contenu. Elles constituent des points de références à partir desquels les autres images sont construites.

– Les images prédites ou *Predicted Pictures* (Images P), ces images sont codées par rapport à une trame I ou P précédente. Elles mettent en œuvre les techniques de compensation de mouvements.

12. NTSC, (*National Television System Committee*) Premier grand système de télévison couleur (1950) utilisé aux Etats Unis et au Japon.

13. PAL (*Phase Alternance Line*), système de télévison couleur d'origine allemande.

© Dunod – La photocopie non autorisée est un délit

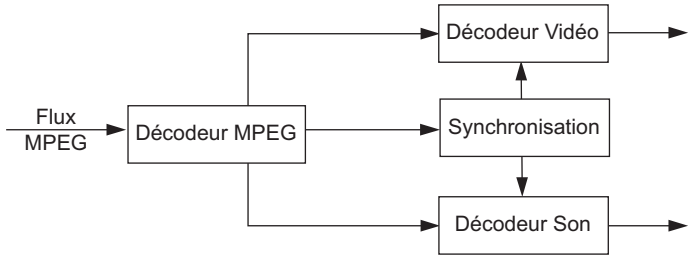


Figure 2.13 Structure fonctionnelle d'un décodeur MPEG.

– Enfin, les images bidirectionnelles ou *Bidirectional Pictures* (Images B), ces images sont déduites non seulement de la précédente, mais aussi de la suivante (prédiction arrière et avant). En effet, s'il est possible de prévoir dans l'image N, d'après l'image N – 1, ce qu'un sujet en mouvement va recouvrir, il n'est pas possible d'estimer ce qu'il va découvrir. À cette fin, cette image utilise l'image N + 1 de type I ou P. Ce qui implique un retard dans la transmission, retard sans importance, l'image télévisuelle n'ayant aucune interactivité avec le téléspectateur.

Des informations temporelles (modulo 24 heures) sont transmises pour mettre à l'heure l'horloge du décodeur (33 bits). À chaque image codée est associée une marque temporelle utilisée par le système pour définir à quel moment il doit afficher l'image.

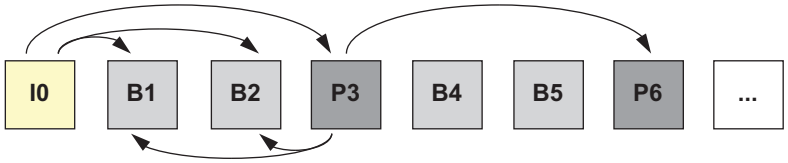


Figure 2.14 Principe de la prédiction d'images dans MPEG.

2.4 NOTION DE QUALITÉ DE SERVICE

2.4.1 Données et contraintes de transmission

Les communications traitent des flux numériques et non des informations. Cependant, selon le type de données les contraintes en termes de débit (volume), de temporalité (temps de transfert et variation de celui-ci) et fiabilité (taux d'erreur) diffèrent.

Ainsi, un transfert de fichier est défini par un flux binaire constant, il requiert un débit relativement important et est très peu sensible au temps de transmission. Plus exigeante en terme de temps de transfert (interactivité), les applications informatiques de type conversationnel sont caractérisées par la sporadicité des flux qu'elles soumettent au système de transmission.

Moins sensible aux erreurs, la voix et la vidéo ont des exigences strictes en matière de débit (débit minimal garanti), de temps de transfert et surtout de récurrence temporelle (gigue),

elles sont qualifiées de données isochrones[14]. La compression opérée sur ces types de données engendre des flux variables. Le tableau de la figure 2.15 résume ces différentes caractéristiques.

Type de transfert	Type de débit	Débit requis	Sensibilité au temps de transfert	Sensibilité aux erreurs
Voix	Constant,	Faible	Élevée (Isochrone)	Faible
Voix compressée	Variable	Faible	Élevée (Isochrone)	Faible
Vidéo non compressée	Constant	Élevée	Élevée (Isochrone)	Faible
Vidéo compressée	Variable	Élevée	Élevée (Isochrone)	Faible
Transactionnel et transfert de fichiers	En rafale (Bursty)	Moyenne à Élevée	Faible	Élevée
Interconnexion de réseaux locaux	En rafale, débit de la source élevé	Élevée	Faible	Élevée

Figure 2.15 Types de données et contraintes de transmission.

2.4.2 Les classes de service

Pour garantir un transfert de données qui respecte les contraintes spécifiques à chaque type de flux de données (transparence sémantique et/ou la transparence temporelle), c'est-à-dire garantir une certaine qualité de service ou **QoS** (*Quality of Service*), le réseau de transport doit déterminer un chemin à travers le réseau qui permette le respect de ces exigences.

Il existe essentiellement deux modes de sollicitation de la qualité de service. La première consiste à faire précéder le transfert de données de l'établissement d'un chemin privilégié. La seconde consiste simplement à marquer le flux et à l'acheminer en fonction des informations de QoS contenues dans chaque bloc de données.

Compte tenu de la combinatoire possible entre les différents éléments de qualité de service, ces derniers ont été regroupés en profils. C'est la notion de classe de service (**CoS**, *Classe of Service*). Plusieurs classifications de CoS ont été définies. La classification formulée par l'ATM[15] Forum est aujourd'hui la seule utilisée. Les classes de service se répartissent en deux catégories, celles qui requièrent une qualité de service multiple (multiservice) comme les applications voix et vidéo et celles de la qualité « données » dont les exigences sont moindres. Les classes de service permettent à l'utilisateur de spécifier ses besoins (contrat de service). Le tableau de la figure 2.16 fournit une description succincte des différentes classes de service.

La classe de service **CBR** (*Constant Bit Rate* ou **DBR**, *Deterministe Bit Rate*) définit un raccordement à débit constant. Elle est destinée aux applications de type voix ou vidéo non compressées.

La classe **VBR** (*Variable Bit Rate* ou **SBR**, *Statistical Bit Rate*) s'applique aux trafics sporadiques, la connexion définit un débit minimal et un débit maximal. Pour les applications temps

14. Isochrone : se dit des flux de données dans lesquels l'écart de temps entre deux informations successives doit être constant. Au cas où le réseau de transmission introduirait un décalage, un mécanisme spécifique doit être mis en œuvre par le récepteur.

15. ATM, *Asynchronous Transfer Mode* ou Mode de Transfert Asynchrone. ATM est une technique d'acheminement des données étudiée spécifiquement pour pouvoir écouler les flux voix, données et images.

© Dunod – La photocopie non autorisée est un délit

Services	Noms	Caractéristiques	Application types
CBR	Constant Bit Rate	Débit constant Flux isochrone	Voix, vidéo non compressée
VBR-rt	Variable Bit Rate real time	Débit variable Flux isochrone	Applications audio et vidéo compressées
VBR-nrt	Variable Bit Rate non real time	Débit variable mais prévisible	Application de type transactionnel
ABR	Available Bit Rate	Débit sporadique Sans contrainte temporelle	Interconnexion de réseaux locaux
UBR	Unspecified Bit Rate	Trafic non spécifié Best Effort	Messagerie, sauvegarde à distance (remote backup)

Figure 2.16 Les classes de service de l'ATM Forum.

réel (**VBR-rt**, *VBR Real Time*), les variations maximales du délai de transfert sont fixées à la connexion. La classe VBR correspond aux applications de type voix ou vidéo compressées.

Les classes CBR et VBR garantissent aux applications une certaine qualité de service, le réseau devant s'adapter aux besoins des applications. Certaines applications, notamment les applications de type données, sont moins exigeantes en terme de débit. Afin de mieux utiliser les capacités du réseau, il semble préférable que ce soient les applications qui s'adaptent aux capacités de transfert de ce dernier et non l'inverse. La classe de service **ABR** (*Available Bit Rate*) ne spécifie, à la connexion, qu'un débit minimal et maximal, il n'y a aucun débit moyen garanti, les applications utilisent le débit disponible sur le réseau (entre les deux bornes prédéfinies).

De même, une classe de service de type datagramme[16] ou *best effort* a été définie : **l'UBR** (*Unspeciefied Bit Rate*). L'UBR ne fournit aucune garantie ni de débit ni de remise des données. Si l'état du réseau le permet, toutes les données introduites dans le réseau sont transmises, en cas de saturation du réseau elles sont éliminées.

2.4.3 Conclusion

La notion de qualité de service est au cœur de la recherche de nouveaux protocoles et des développements des réseaux. Des solutions ont été apportées à ce problème dans les protocoles de dernières générations tels qu'**ATM** (*Asynchronous Transfer Mode*), tandis que les protocoles plus anciens comme **TCP/IP** (*Transmission Control Protocol/Internet Protocol*) ont été adaptés et enrichis pour en tenir compte.

16. Un datagramme est une unité de données constituant un tout et acheminé tel quel sur le réseau sans aucune garantie de délivrance.

EXERCICES

Exercice 2.1 Code ASCII, Algorithme de changement de casse

Donner l'algorithme qui transforme la chaîne (String) codée en ASCII : Chaine = "IL FAIT BEAU", en chaîne : ASCII Chaine = "il fait beau", en pseudo-code et dans le langage de votre choix (Pascal, C).

Exercice 2.2 Codage de Huffman

Deux terminaux informatiques s'échangent des messages de longueur moyenne égale à 2 000 caractères. Ces caractères, clairement identifiés (A, F, O, R, U, W), apparaissent avec des probabilités respectives suivantes : 0,23 - 0,09 - 0,30 - 0,19 - 0,14 - 0,05.

On vous demande :

– de déterminer la longueur du code idéal ;

– de construire l'arbre d'Huffman, puis de donner le code correspondant pour chacun des caractères ainsi que le nombre de bits du message ainsi codé ;

– de calculer la longueur moyenne du code établi ;

– d'évaluer le taux de compression obtenu par rapport au code Baudot ;

– enfin, sachant que le signal est transmis sur un support dont le débit de 4 800 bit/s, quel est le temps de transmission du message codé en ASCII et selon le code que vous aurez établi ?

Exercice 2.3 Télécopieur

Dans un télécopieur, un scanner analyse l'image ligne par ligne (balayage horizontal). Chaque ligne est découpée en un certain nombre de points (pixel). L'analyse de la ligne se traduit par une suite, plus ou moins longue, de zones blanches ou noires (séquence). La redondance d'information peut être réduite en ne transmettant que les informations de longueur et non les séquences elles-mêmes. Le codage des informations, en télécopie groupe 3, utilise le principe du code Huffman (code à longueur variable) appelé : code Huffman Modifié (HM). À chaque longueur de séquence de blancs ou de noirs est associée un mot binaire unique. Sur ce principe, on vous demande de coder en Huffman le texte ci-dessous (figure 2.17).

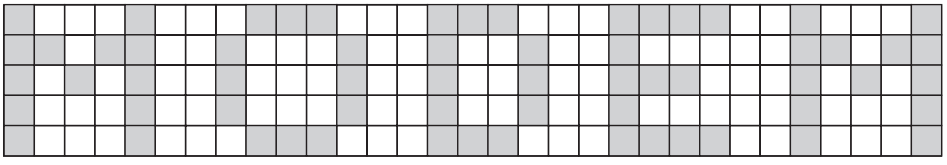


Figure 2.17 Page à coder en Huffman.

© Dunod – La photocopie non autorisée est un délit

Exercice 2.4 Numérisation du son

Les CD audios échantillonnent le son à 44,1 kHz et le quantifient sur 16 bits. Pour améliorer la qualité de restitution, deux nouvelles technologies s'affrontent. Le DVD audio qui échantillonne à 192 kHz et quantifie sur 24 bits, tandis que le SACD analyse le son à raison de 2,8224 MHz et quantifie la variation sur 1 bit. On vous demande de calculer :

– le débit nécessaire pour qu'une ligne transmette en temps réel les flux audios ;

– en négligeant les données de service (correction d'erreur, index...), le volume à stocker pour une œuvre musicale d'une durée d'une heure.

Exercice 2.5 Numérisation et débit binaire

La télévision analogique occupe une largeur de bande de 6,75 MHz pour l'information de luminance et une bande réduite de moitié pour les informations de chrominance. Chaque signal étant quantifié sur 8 bits, on vous demande :

– Quel débit binaire serait nécessaire pour transmettre ces images numérisées ?

– Quel serait le nombre de couleurs de l'image ainsi numérisée ?

Exercice 2.6 Rapport signal à bruit et loi de quantification A

La loi de quantification logarithmique A permet d'obtenir un rapport signal à bruit pratiquement constant sur tout l'espace de quantification. En établissant pour chaque segment de quantification la valeur maximale du bruit de quantification, vérifiez, de manière simple, cette assertion.

Exercice 2.7 Image RVB

Deux solutions étaient envisageables pour la télévision numérique, transmettre une image RVB ou une image Y, Db et Dr. Quel est l'avantage de la deuxième solution en matière d'efficacité de la transmission ?

Chapitre **3**

Éléments de base de la transmission de données

Transporter de l'information d'un point à un autre nécessite que soit établie une série de conventions concernant la représentation logique des données (chapitre précédent), les paramètres physiques de la transmission (niveau électrique, rythme de l'émission...) et le mode de contrôle de l'échange. Cet ensemble de conventions constitue le protocole[1] de transmission, il qualifie une transmission et définit ses possibilités d'emploi.

3.1 CLASSIFICATION EN FONCTION DU MODE DE CONTRÔLE DE L'ÉCHANGE

3.1.1 Selon l'organisation des échanges

La transmission d'information entre deux correspondants peut être unidirectionnelle (l'échange n'a lieu que dans une seule direction), on parle alors de **liaison simplex** (figure 3.1). Chaque correspondant ne remplit qu'une fonction, il est émetteur (source) ou récepteur (puits ou collecteur).

Si les correspondants peuvent, alternativement, remplir les fonctions d'émetteur et de récepteur, la liaison est dite : liaison à l'**alternat** ou *half duplex*. Le temps mis par les systèmes pour passer d'une fonction à l'autre est appelé temps de retournement. Ce temps peut être important, jusqu'à 1/3 de seconde.

1. Le terme protocole est employé ici dans un sens large. La notion de protocole de transmission est plus restrictive, le principe des protocoles de transmission fera l'objet de l'étude du chapitre 6.

Lorsque l'échange peut s'effectuer simultanément dans les deux sens, sur des voies distinctes ou sur la même voie par utilisation de techniques spécifiques comme le multiplexage fréquentiel[2], la liaison est appelée **bidirectionnelle intégrale** ou *full duplex*.

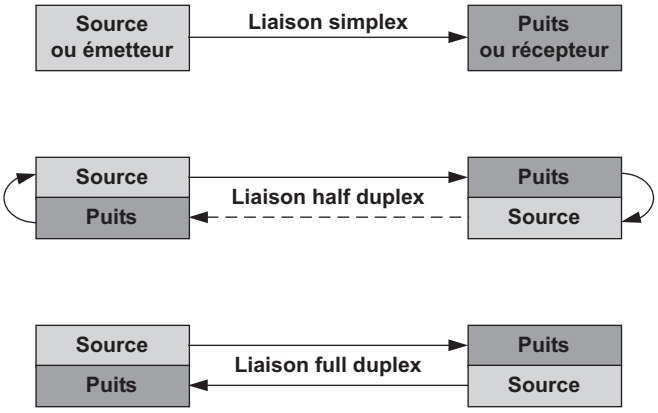


Figure 3.1 Organisation des échanges.

3.1.2 Selon le mode de liaison

La liaison point à point

Dans ce mode de liaison chaque correspondant est relié par un lien dédié à un seul autre correspondant. C'est le cas par exemple d'une liaison entre nœuds[3] d'un même réseau ou entre un ordinateur et un terminal (figure 3.2).

Figure 3.2 La relation point à point.

Les liaisons multipoints

Une liaison est dite **multipoint** lorsqu'un même support est partagé par plusieurs nœuds. Dans ce cas, des conflits d'accès sont inévitables, il est nécessaire d'instaurer une politique d'accès au support. L'ensemble des mécanismes particuliers mis en œuvre, pour assurer le partage de l'accès au support, porte le nom de politique d'accès au canal On distingue deux modes de contrôle de l'accès selon la manière dont est gérée la politique d'accès : le mode centralisé ou maître/esclave et le mode décentralisé ou d'égal à égal.

➤ Le mode maître/esclave

Dans le mode de relation dit maître/esclave (figure 3.3) le primaire, généralement un ordinateur multipostes (*mainframe* ou mini-ordinateur) est responsable de l'initialisation du dialogue, de

2. Le multiplexage fréquentiel consiste à utiliser une fréquence différente pour chaque voie de communication (voir chapitre 7, *Mutualisation des ressources*).

3. Le terme nœud (*node*) désigne d'une manière générale tout calculateur qui reçoit, émet et/ou traite des données.

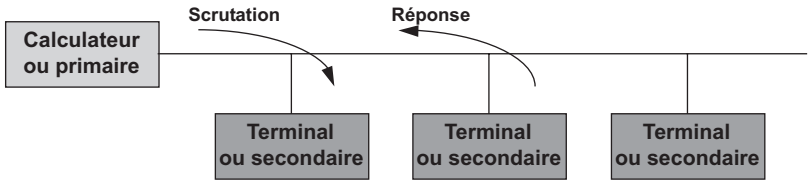


Figure 3.3 La relation maître/esclave.

la récupération des erreurs et de l'organisation des échanges. Le transfert des données s'effectue selon la technique dite du « *polling/selecting* » (figure 3.4). Le maître invite le terminal (secondaire) à émettre (*polling*) ou lui demande de passer en mode réception (*selecting*).

Dans de grandes configurations, le polling de toutes les stations peut demander beaucoup de temps. Pour améliorer les temps de réponse, on utilise la technique dite du *polling* lent et *polling* rapide. À l'initialisation, toutes les stations sont interrogées, ensuite uniquement celles qui ont répondu (*polling* rapide) ; périodiquement, toutes les stations sont de nouveau interrogées (*polling* lent).

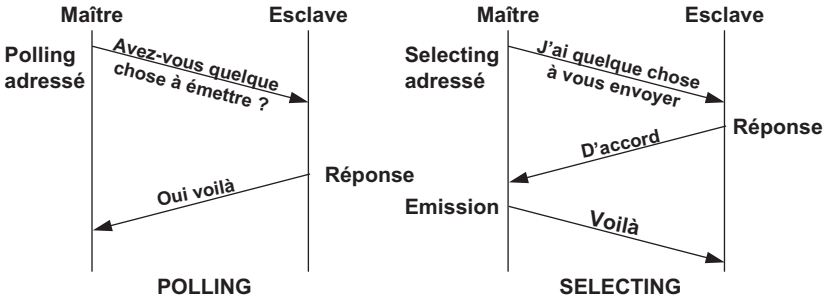


Figure 3.4 Polling/Selecting.

➤ Le mode d'égal à égal

Dans ce type de configuration, tous les calculateurs sont autorisés à émettre vers n'importe quel autre calculateur et ce, à tout moment. Cet accès partagé peut donner lieu à des collisions ou contentions de messages (deux stations transmettent en même temps). Mais contrairement à la relation maître/esclave, ici, chaque calculateur déroule un algorithme pour assurer le partage du support. La politique d'accès est dite décentralisée. Les réseaux locaux[4] constituent un exemple de ce mode de contrôle de l'accès au support.

3.1.3 Les modes de contrôle de la liaison

Pour établir une communication, l'un des correspondants doit initialiser la transmission. Durant toute la transmission, en sus des données, des informations de contrôle sont échangées. On distingue différents modes de contrôle de la liaison selon celui qui peut prendre l'initiative d'une transmission et celui qui la contrôle.

4. Voir chapitre 12, *Les réseaux locaux*.

© Dunod – La photocopie non autorisée est un délit

La dissymétrie synchrone

La dissymétrie synchrone est utilisée dans la relation maître/esclave ou polling du primaire vers le secondaire. Ce mode, mis en œuvre dans les liaisons multipoint, est appelé *Normal Response Mode* (**NRM**) ou *Link Access Protocol* (**LAP**).

La symétrie synchrone

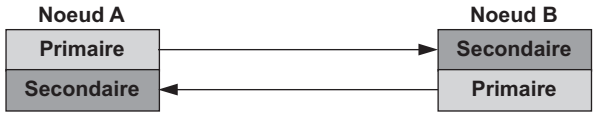


Figure 3.5 La symétrie synchrone.

Dans les communications en point en point, la symétrie synchrone permet, à chaque extrémité, d'être primaire en émission et secondaire en réception (figure 3.5). Connue sous le nom de mode équilibré ou *Asynchronous Balanced Mode* (**ABM**), elle est employée dans les liaisons *full duplex* (*Link Access Protocol Balanced* ou **LAP B**) et *half duplex* (**LAP X**, *LAP semi-dupleX*).

La dissymétrie asynchrone

Dans ce mode, le secondaire peut émettre sans y avoir été autorisé. Ce qui implique qu'un seul secondaire puisse être actif à la fois ou qu'un algorithme de résolution des collisions soit mis en œuvre. Ce mode est appelé *Asynchronous Response Mode* (**ARM**).

3.2 CLASSIFICATION EN FONCTION DES PARAMÈTRES PHYSIQUES

3.2.1 Transmission parallèle, transmission série

L'information élémentaire à transmettre est le mot (4, 8, 16, *n* bits). En interne, les calculateurs transfèrent les données via un bus : un fil par bit. Le bus transmet simultanément tous les bits d'un même mot machine, la transmission est dite transmission parallèle, la communication entre machines peut se réaliser de même. La transmission parallèle soulève de nombreux problèmes techniques. Pour des distances importantes, on lui préfère la transmission série : les bits sont transmis successivement sur un support unique.

Transmission parallèle

La transmission parallèle (figure 3.6) est caractérisée par un transfert simultané de tous les bits d'un même mot. Elle nécessite autant de conducteurs qu'il y a de bits à transmettre et un conducteur commun (liaison asymétrique) ou autant de paires de fils si la masse n'est pas commune (liaison symétrique).

La transmission parallèle est très performante en terme de débit. Elle est utilisée pour des liaisons entre un calculateur, ses périphériques et ses unités de calcul esclaves. Par exemple, l'interface **HiPPI** (*High Performance Parallel Interface*) qui définit un mode de transmission entre un calculateur et ses périphériques offre un débit de 800 Mbit/s. Elle utilise un câble de

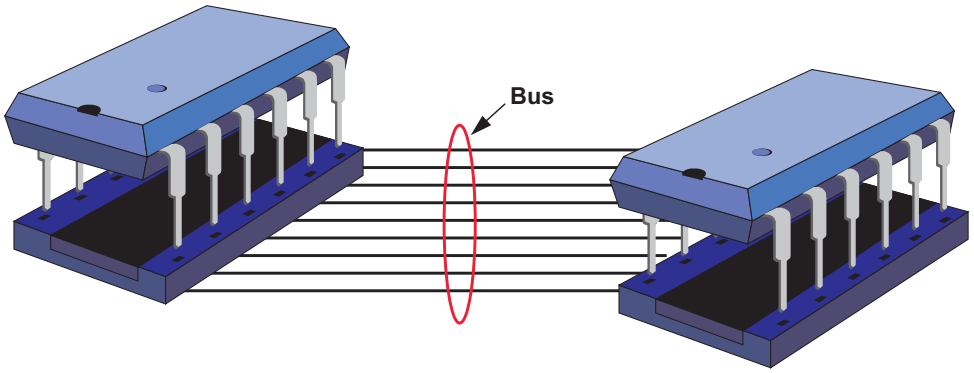


Figure 3.6 La transmission parallèle.

50 paires dont 32 sont utilisées pour la transmission de données (transmission parallèle par mot de 32 bits). HiPPI est limitée à 25 m.

La transmission parallèle pose de nombreuses difficultés dont les principales sont le rayonnement des conducteurs l'un sur l'autre (diaphonie[5]) et la différence de vitesse de propagation entre les différents conducteurs (*Delay Skew*) qui nécessitent la réalisation d'une électronique coûteuse.

Un coût élevé (nombre de conducteurs) et une distance franchissable limitée par la désynchronisation du train de bits (*Delay Skew*) réservent la transmission parallèle aux liaisons de processeur à processeur ou d'hôte à hôte (ordinateur central). Des techniques apparentées sont mises en œuvre dans les réseaux locaux.

Transmission série

En transmission série (figure 3.7), tous les bits d'un mot ou d'un message sont transmis successivement sur une même ligne.

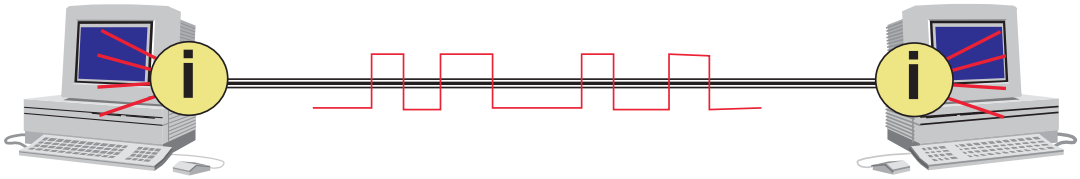


Figure 3.7 Transmission série.

Dans les calculateurs, les données (bits) sont traitées en parallèle (bus). La transmission série nécessite une interface de conversion pour sérialiser les bits en émission (conversion parallèle/série) et les désérialiser en réception (conversion série/parallèle). La transmission série n'utilise, pour la transmission des données, que deux conducteurs. D'un coût moins élevé, elle est adaptée aux transmissions sur des distances importantes.

5. Voir chapitre 4, *Les supports de transmission*.

© Dunod – La photocopie non autorisée est un délit

Comparaison

Si on désigne par **temps bit** le temps d'émission d'un bit sur le support, en considérant que ce temps est identique pour la transmission parallèle et série de la figure 3.8, on constate qu'il faut seulement 3 temps bit pour transmettre le mot « ISO » en transmission parallèle, alors que la transmission série nécessite 8 temps bit pour transmettre la seule lettre « O ».

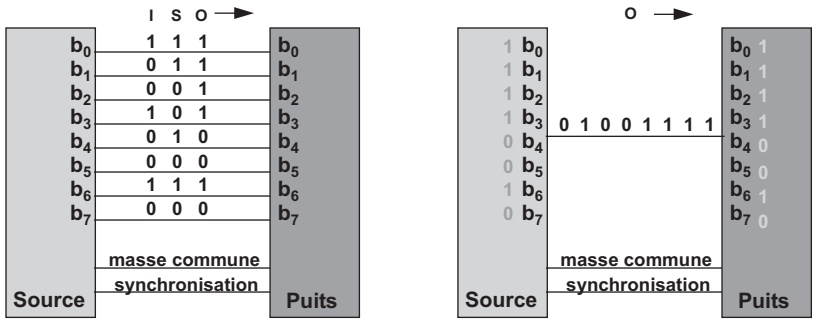


Figure 3.8 Transmission parallèle, transmission série.

3.2.2 Transmission asynchrone, transmission synchrone

Les bits sont émis sur la ligne à une certaine cadence. Cette cadence est définie par une horloge dite horloge émission. Pour décoder correctement la suite de bits reçue, le récepteur doit examiner ce qui lui arrive à une cadence identique à celle de l'émission des bits sur le support. Les horloges récepteur et émetteur doivent « battre » en harmonie.

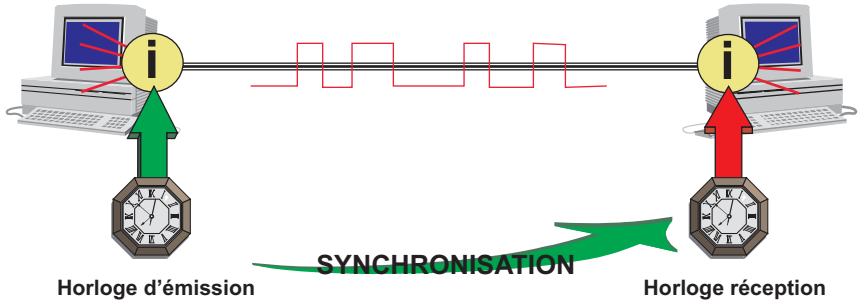


Figure 3.9 Principe de la synchronisation.

Il ne suffit pas que les horloges battent au même rythme, encore faut-il que les instants d'analyse des niveaux électriques de la ligne soient les mêmes pour les deux éléments, ils sont dits en phase. L'opération qui consiste à asservir l'horloge de réception sur celle d'émission s'appelle la synchronisation (figure 3.9). Selon le mode de synchronisation de l'horloge du récepteur sur celle de l'émetteur, on distingue deux types de transmission : les transmissions asynchrones et les transmissions synchrones.

Dans les transmissions asynchrones les horloges sont indépendantes ; au contraire, dans les transmissions synchrones on maintient en permanence une relation de phase stricte entre les horloges émission et réception.

Lorsque les systèmes terminaux sont reliés via un réseau de transport, c'est ce dernier qui fournit les horloges de référence (figure 3.10).

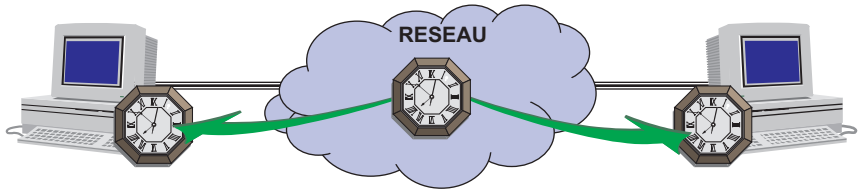


Figure 3.10 Synchronisation des horloges sur l'horloge réseau.

Notion d'horloge

La synchronisation des différentes horloges mises en œuvre dans les systèmes de transmission est l'une des préoccupations principales des concepteurs de systèmes de transmission. Les dérives d'horloge et, par conséquent, les pertes de synchronisation sont, aujourd'hui, les principales causes des pertes de données et des erreurs de transmission dans les réseaux.

Les bits sont émis au rythme de l'horloge locale de l'émetteur que nous supposons stable. L'horloge du récepteur est supposée fonctionner à la même cadence ou fréquence (nombre d'instants significatifs par seconde identique). Cependant, rien ne permet de garantir sa stabilité. La fréquence varie, on dit que l'horloge dérive. En admettant que lors de la réception du premier bit, l'horloge du récepteur soit parfaitement calée sur l'horloge d'émission (synchronisée), la dérive de l'oscillateur local du récepteur fait que quelques bits plus tard, l'instant significatif de lecture est sur le bit suivant ou précédent selon le sens de la dérive. En admettant (hypothèse simplificatrice), que l'instant d'interprétation du signal reçu corresponde au front descendant de l'horloge de réception, la dérive illustrée figure 3.11 (dérive positive) montre que, du fait de cette dernière, le cinquième bit est omis. Une erreur de transmission est apparue.

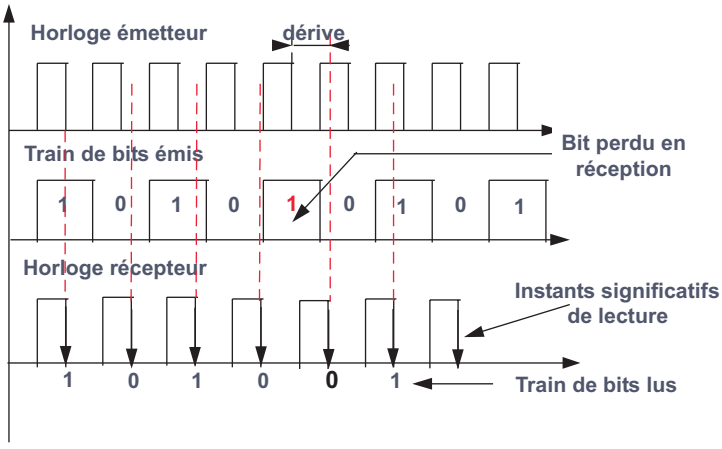

Horloge émetteur
dérive
Train de bits émis
Bit perdu en réception
1 0 1 0 1 0 1 0 1
Horloge récepteur
Instants significatifs de lecture
1 0 1 0 0 1
Train de bits lus

Figure 3.11 La dérive de l'horloge réception occasionne la perte d'un bit.

Le signal de synchronisation peut être transmis sur un lien spécifique ou déduit du train binaire. La première méthode plus complexe et plus onéreuse est utilisée par les opérateurs de

© Dunod – La photocopie non autorisée est un délit

télécommunication pour transmettre la synchronisation aux différents éléments du réseau. En général, les équipements terminaux utilisent la seconde méthode, le signal d'horloge est extrait du train binaire transmis.

La figure 3.12 montre le principe de l'extraction, à partir du train numérique reçu, d'un signal de pilotage de l'oscillateur local (horloge locale).

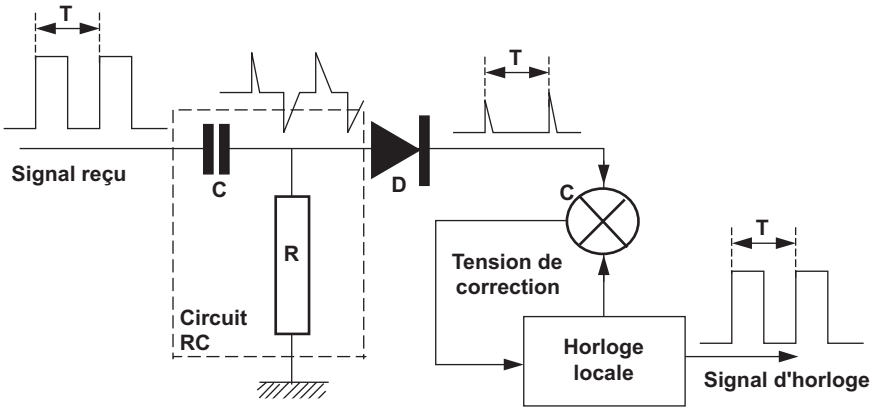


Figure 3.12 Principe d'asservissement de l'horloge du récepteur.

Transmission asynchrone

Dans les transmissions asynchrones, les horloges émetteur et récepteur sont indépendantes. Pour assurer la synchronisation des horloges on envoie, avant toute suite binaire significative, un signal spécifique d'asservissement. Après cette opération, l'horloge de réception est libre, elle dérive. L'intervalle de temps, pendant lequel la dérive est tolérable et autorise un décodage correct de la séquence binaire, est faible. Cet intervalle de temps n'autorise que la transmission d'une courte séquence binaire : le caractère.

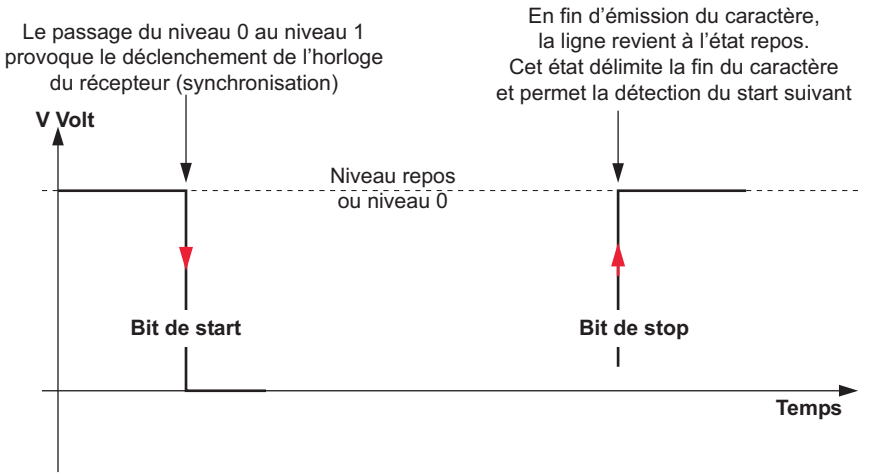

Le passage du niveau 0 au niveau 1
provoque le déclenchement de l'horloge
du récepteur (synchronisation)
En fin d'émission du caractère,
la ligne revient à l'état repos.
Cet état délimite la fin du caractère
et permet la détection du start suivant
V Volt
Niveau repos
ou niveau 0
Bit de start
Bit de stop
Temps

Figure 3.13 Principe de la synchronisation en transmission asynchrone.

En transmission asynchrone, les caractères émis sont précédés d'un signal de synchronisation : le **bit de start**. Entre chaque caractère, pour garantir la détection du bit de start suivant, la ligne est remise à l'état zéro. Ce temps de repos minimal varie de 1 à 2 temps bit, il constitue le ou les **bits de stop** (figure 3.13). Le niveau de repos de la ligne ou niveau zéro est fixé à un certain potentiel (V) et non pas au zéro électrique pour ne pas confondre un zéro binaire avec une rupture de la ligne. Cette tension de repos signale aux systèmes que les terminaux sont actifs.

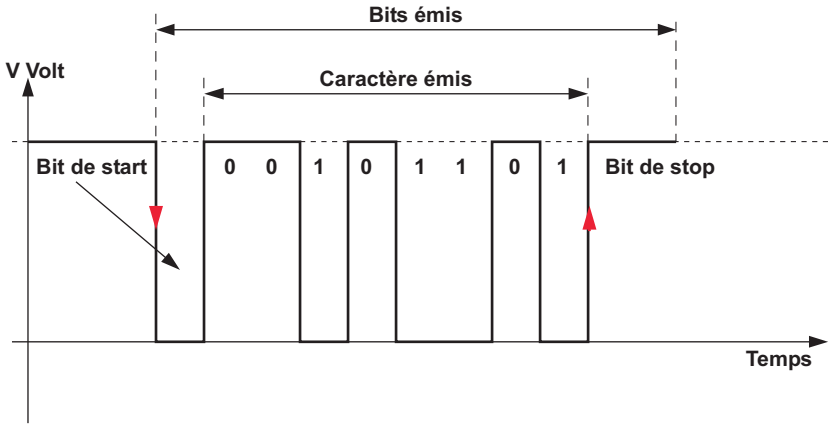


Figure 3.14 Caractère asynchrone.

Le bit de start et celui ou ceux de stop servent de délimiteur de caractères (figure 3.14). Les transmissions asynchrones s'effectuent selon un ensemble de règles régissant les échanges (protocole). On distingue deux types de protocoles asynchrones (figure 3.15) :

– Le mode caractères : la transmission a lieu caractère par caractère. L'intervalle de temps qui sépare chaque caractère peut être quelconque (multiple de la fréquence d'horloge).

– Le mode blocs : les caractères sont rassemblés en blocs. L'intervalle de temps entre l'émission de 2 blocs successifs peut être quelconque (multiple de la fréquence d'horloge).

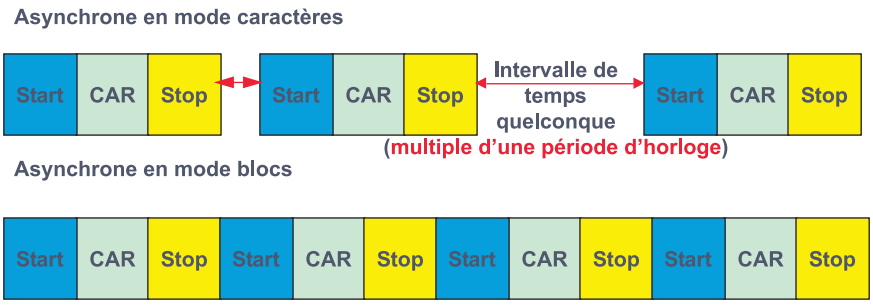

Asynchrone en mode caractères
Start CAR Stop
Start CAR Stop
Intervalle de temps quelconque
(multiple d'une période d'horloge)
Start CAR Stop
Asynchrone en mode blocs
Start CAR Stop Start CAR Stop Start CAR Stop Start CAR Stop

Figure 3.15 Mode caractères et mode blocs.

Le principe des protocoles de transmission sera étudié au chapitre 6. Les principaux protocoles asynchrones sont :

– **XON-XOFF**, protocole orienté caractères, le terminal réactive la ligne quand il est prêt à émettre, il la désactive quand il n'a plus de données disponibles ;

© Dunod – La photocopie non autorisée est un délit

– **X-Modem**, protocole orienté blocs, les caractères sont regroupés en blocs. Ce protocole du domaine public met en œuvre des techniques de détection et reprise sur erreur ;
– **Y-Modem**, protocole orienté blocs, les blocs de données sont suivis de code de détection d'erreur. Aucune reprise sur erreur n'est assurée ;
– **Z-Modem**, protocole orienté blocs, il met en œuvre des mécanismes de détection et de reprise automatique sur erreur ;
– **SLIP** (*Serial Line Internet Protocol*), protocole orienté blocs. Très simple, SLIP n'effectue que la délimitation des blocs ;
– **PPP** (*Point to Point Protocol*) protocole orienté blocs, PPP effectue la délimitation des blocs et la détection d'erreur.

Transmission synchrone

En transmission synchrone, la synchronisation des horloges émission et réception est maintenue durant toute la transmission par un signal particulier : le signal de synchronisation. Il est alors possible de transmettre des blocs de taille importante. Cependant, entre chaque bloc transmis, l'horloge réception n'est plus pilotée et dérive. Chaque bloc transmis est par conséquent précédé d'une séquence de synchronisation qui servira aussi à délimiter le début et la fin de bloc (figure 3.16).

Figure 3.16 Structure type d'un bloc de données en transmission synchrone.

À la réception, le récepteur doit être capable de se positionner correctement pour la lecture des bits. Cette opération de synchronisation des horloges est réalisée à l'aide d'une séquence de bits contenant un grand nombre de transitions (synchronisation bit). Puis, il doit identifier les différents caractères transmis (alignement de la lecture sur des frontières de mots ou synchronisation caractère).

Dans la procédure **BSC** (*Binary Synchronous Communication*), le caractère utilisé pour ces fonctions est le caractère ASCII SYN « 0010110 ». En réception, la lecture du flot de bits arrivant s'effectue dans un registre à décalage contenant autant de bits que le caractère à lire en comporte. Chaque bit qui arrive est introduit dans le registre en poussant le premier bit entré ; enfin, on examine le mot contenu dans le registre pour y rechercher le caractère SYN. Lorsqu'une station reconnaît ce caractère, elle positionne les frontières de caractère en se basant sur le caractère reconnu (synchronisation caractère).

Les principaux protocoles synchrones sont :

– **BSC**, *Binary Synchronous Communication* (IBM) ;
– **SDLC**, *Synchronous Data Link Control* (IBM) ;
– **HDLC**, *High Level Data Link Control* (ISO) ;
– **PPP**, *Protocol Point to Point*, ce dernier est aussi un protocole asynchrone (IETF).

Illustration des modes de transmission

La figure 3.17 illustre les différents modes de transmission. Dans la liaison de gauche, chaque caractère introduit au clavier est immédiatement transmis à l'ordinateur central. L'ordinateur maître acquitte le caractère en le renvoyant au terminal qui l'affiche (écho). Dans ce type de liaison, les caractères sont émis sur le support au rythme de la frappe, il n'y a aucun lien temporel entre eux. La transmission est arythmique, le terminal est qualifié d'asynchrone. Le principal avantage de ce mode de relation est la simplicité du terminal et du protocole d'échange ; la détection et la correction d'erreur sont notamment réalisées par l'opérateur. Le Minitel et le VT100 sont des exemples de ce type de terminal.

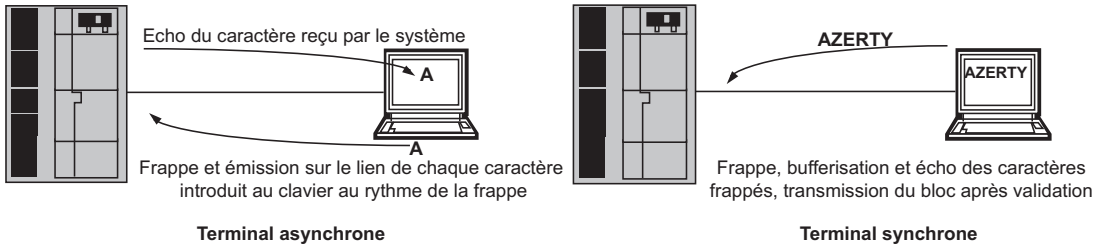

Echo du caractère reçu par le système
A
A
Frappe et émission sur le lien de chaque caractère introduit au clavier au rythme de la frappe
Terminal asynchrone
AZERTY
AZERTY
Frappe, bufferisation et écho des caractères frappés, transmission du bloc après validation
Terminal synchrone

Figure 3.17 Terminaux et mode de transmission.

Dans le schéma de droite, les données introduites au clavier sont affichées directement (écho local) et mémorisées. Lorsque l'opérateur valide la saisie, l'ensemble des données saisies est transmis. Le bloc de données émis peut être important, il est alors nécessaire de synchroniser en permanence le destinataire sur la source (transmission synchrone). Le lien de transmission est mieux utilisé, la transmission est plus performante mais le terminal est plus complexe. Notamment, le protocole de transmission doit permettre au calculateur destinataire de détecter toutes les erreurs de transmission.

Comparaison

Une liaison de données est caractérisée par son débit (D) qui représente le nombre de bits transmis par unité de temps (bit/s). Cependant, il convient de distinguer le débit nominal (*Dn*) qui correspond au nombre de symboles binaires que le système est susceptible de transmettre, du débit réel (*Dr*) ou effectif qui mesure le nombre de bits utiles émis sur le support durant le temps réel de la session de transfert ramené à l'unité de temps. Le rapport de ces deux grandeurs mesure l'efficacité du système (*Eff*).

$$Eff = \frac{Dr}{Dn}$$

Le protocole PPP (*Point to Point Protocol*), utilisé pour l'accès à Internet, fonctionne en mode asynchrone et en mode synchrone. Lors de la connexion, pour un obtenir un fonctionnement optimal, une phase de négociation permet de configurer PPP. En admettant que, dans les deux cas, cette phase ait défini l'utilisation de la trame standard, notamment une charge utile de 1 500 octets, quelle est l'efficacité de ce protocole dans les deux modes de fonctionnement ? La figure 3.18 représente la trame PPP ; la signification des différents champs sera précisée lors de l'étude de ce protocole.

© Dunod – La photocopie non autorisée est un délit

Fanion 0x7E	Adresse 0xFF	Contrôle UI = 0x	Protocole 2 octets	Données 1 500 octets	FCS 2 octets	Fanion 0x7E

Figure 3.18 Trame PPP.

La trame PPP (figure 3.18) comporte 8 octets de service[6] (2 fanions d'un octet, 1 octet pour le champ adresse, 1 pour le champ contrôle, 2 pour le champ protocole et 2 pour le champ FCS) pour une charge utile de 1 500 octets d'information (*payload*).

L'efficacité dans le mode synchrone correspond au rapport du nombre d'octets utiles au nombre d'octets transmis soit :

$$Eff = \frac{1500}{1508} = 0{,}994$$

En mode asynchrone, il faut, à chaque octet ajouter un bit de start et un bit de stop soit 10 bits pour 8 d'utiles. L'efficacité dans ces conditions est :

$$Eff = \frac{1500 \cdot 8}{1508 \cdot 10} = 0{,}795$$

Essentiellement pour des raisons de dérive d'horloge et d'efficacité, les systèmes de transmission à bas débit constituent le domaine de prédilection du mode asynchrone. Cependant, compte tenu des coûts plus faibles des systèmes asynchrones par rapport aux coûts des systèmes synchrones, ils sont mis en œuvre dans les systèmes grand public pour les accès à Internet à 56 000 bit/s via le réseau téléphonique commuté.

Attention : les termes synchrone et asynchrone ont, selon ce qu'ils qualifient, des significations différentes. Un tableau en annexe résume les différentes utilisations de ces termes dans le monde des télécommunications.

3.2.3 Selon le mode de transmission électrique

Les zéros ou les uns sont différentiés par un niveau électrique différent. On distingue deux modes selon la manière dont sont lus les niveaux électriques.

Le mode dissymétrique

Dans le mode asymétrique (ou dissymétrique), l'information d'état est fournie par la différence de potentiel entre le conducteur concerné et un conducteur de retour. Le fil de retour peut être commun à plusieurs fonctions. Ce conducteur commun est souvent désigné sous le terme de **terre de signalisation**. La figure 3.19 représente les variations de potentiel (+V, −V) autour d'une valeur de référence dite « zéro électrique ».

Ce mode de transmission est simple à réaliser au niveau de l'électronique, il ne nécessite que 2 conducteurs mais est très sensible aux parasites.

Le mode symétrique

Dans le mode symétrique appelé aussi **transmission différentielle**, l'information d'état est déduite de la différence de potentiel entre deux conducteurs. La figure 3.20 illustre ce mode de

6. Pour la signification de chacun de ces champs voir chapitre 6.

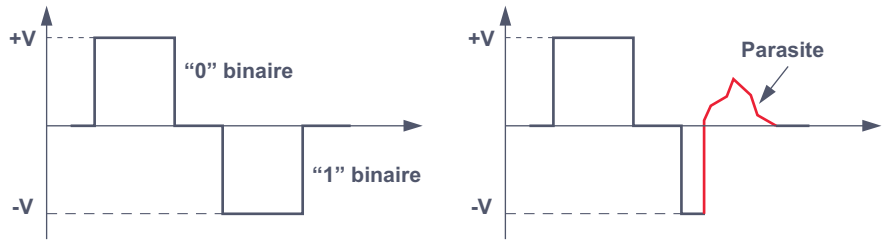


Figure 3.19 Transmission asymétrique.

transmission. À l'état repos, chaque conducteur est, par exemple, au potentiel + Volt par rapport à une référence commune, la différence de potentiel entre ces conducteurs est nulle (repère 1). Pour transmettre une information binaire, chacun des conducteurs voit son potentiel évoluer en sens inverse (repère 2 et 3) de la figure 3.20.

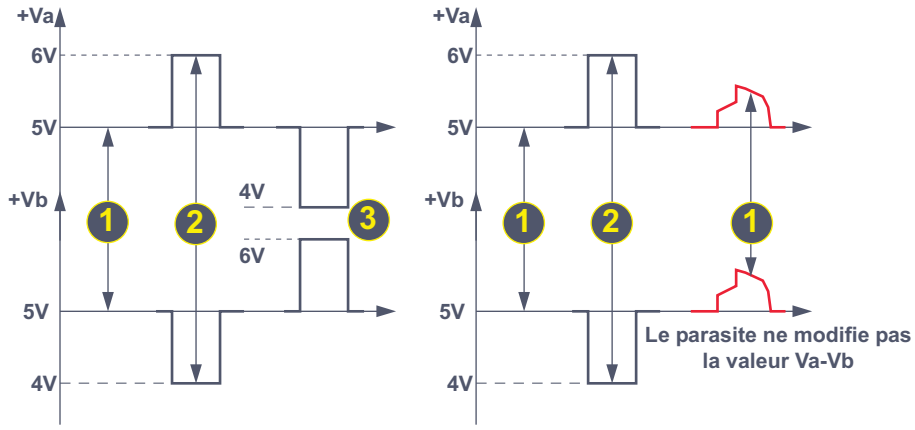


Figure 3.20 Transmission symétrique ou différentielle.

En 1, position de repos, la tension lue (Va − Vb) est nulle. En 2, l'expression Va − Vb = 6 − 4 = 2 V c'est par exemple le niveau 0 ; alors qu'en 3, Va − Vb = 4 − 6 = −2 V pourrait représenter le 1 binaire. Ce mode de représentation, plus complexe, nécessite plus de conducteurs mais un parasite électrique ne modifie pas le niveau relatif. La transmission présente une certaine insensibilité aux parasites.

3.3 PRINCIPE D'UNE LIAISON DE DONNÉES

Une transmission de données met en œuvre des calculateurs d'extrémité et des éléments d'interconnexion dont les appellations et fonctions sont codifiées (figure 3.21) :

On distingue :

– Les équipements terminaux (*End System*) ou **ETTD**, Équipement Terminal de Traitement de Données, appelés aussi **DTE** (*Data Terminal Equipement*) représentant les calculateurs d'extrémité. Ces calculateurs sont dotés de circuits particuliers pour contrôler les communications. L'ETTD réalise la fonction de contrôle du dialogue.

© Dunod – La photocopie non autorisée est un délit

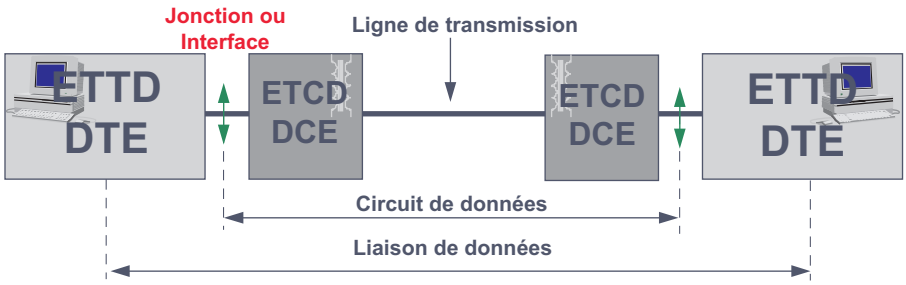


Figure 3.21 Constituant de base d'une liaison de données.

– Des équipements d'adaptation ou **ETCD**, Équipement Terminal de Circuit de Données, ou **DCE** (*Data Communication Equipement*) réalisent l'adaptation entre les calculateurs d'extrémité et le support de transmission. Cet élément remplit essentiellement des fonctions électroniques, il assure un meilleur transport sur la ligne de transmission. Il modifie la nature du signal, mais pas sa signification.

– La jonction constitue l'interface entre ETTD (DTE) et ETCD (DCE), elle permet à l'ETTD de gérer l'ETCD pour assurer le déroulement des communications (établissement du circuit, initialisation de la transmission, échange de données et libération du circuit).

– Le support ou ligne de transmission est un élément essentiel de la liaison. Les possibilités de transmission (débit, taux d'erreur...) dépendent essentiellement des caractéristiques physiques et de l'environnement de celui-ci.

Les deux chapitres suivants sont consacrés à l'étude de ces différents éléments. Après l'étude des supports et de leur influence sur la transmission, on examinera comment est réalisée l'adaptation du signal à ces supports. Ce dernier point nous conduira à distinguer deux modes physiques de transmission : la transmission dite en bande de base (*Baseband Transmission*) et la transmission par transposition de fréquence ou large bande (*Broadband Transmission*).

EXERCICES

Exercice 3.1 Organisation des échanges

Donnez un exemple de la vie courante pour chacun des modes de contrôle des échanges.

Exercice 3.2 Transmission parallèle

Combien de conducteurs sont nécessaires pour réaliser une transmission en parallèle de mots machines de 32 bits si on utilise ou non un retour commun ?

Exercice 3.3 Transmission synchrone et asynchrone

Rappeler brièvement ce qui distingue ces deux modes de transmission.

Exercice 3.4 Élément d'accès aux réseaux

Un DTE peut-il être raccordé directement au réseau d'un opérateur ?

Exercice 3.5 Transmission asynchrone

En transmission asynchrone, l'horloge du récepteur n'est synchronisée qu'en début de transmission. Une source a une horloge de 1 000 Hz (1 000 bit/s) avec une stabilité de 10^{-2}. Sachant que pour lire correctement un bit on ne peut admettre qu'une dérive maximale de 10 % par rapport à un temps bit et que le débit binaire est égal à la rapidité de modulation, quel est le nombre de bits que l'on peut émettre en une fois ?

Exercice 3.6 Durée d'un transfert d'information

Une entreprise désire réaliser la sauvegarde de ses données sur un site distant. Le volume de données à sauvegarder est estimé à 10 Go/jour. La sauvegarde doit s'effectuer la nuit de 22 h 00 à 6 h 00. Les deux sites sont reliés par une ligne à 2 Mbit/s. On vous demande de vérifier si cette solution est réalisable et le cas échéant de proposer une solution qui permette cette sauvegarde. Pour ce problème on admettra que 1ko = 1 000 octets.

© Dunod – La photocopie non autorisée est un délit

Chapitre **4**

Les supports de transmission

L'infrastructure d'un réseau, la qualité de service offerte, les solutions logicielles à mettre en œuvre dépendent largement des supports de transmission utilisés. Les supports de transmission exploitent les propriétés de conductibilité des métaux (paires torsadées, coaxial), celles des ondes électromagnétiques (faisceaux hertziens, guides d'onde, satellites) ou encore celles du spectre visible de la lumière (fibre optique). Généralement on classe les supports en deux catégories :

– les supports guidés (supports cuivre et supports optiques) ;
– les supports libres (faisceaux hertziens et liaisons satellites).

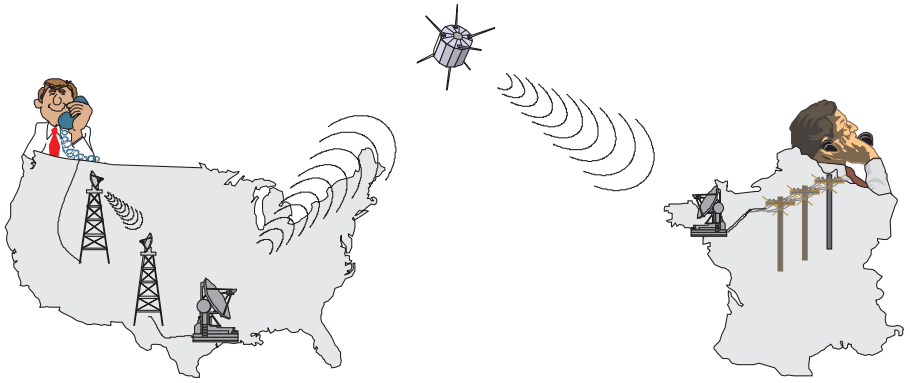


Figure 4.1 Une liaison informatique peut mettre en œuvre plusieurs types de support.

La complexité des systèmes provient généralement du fait qu'une liaison peut emprunter différents supports (figure 4.1). Le système de transmission devra alors réaliser l'adaptation du signal à transmettre au support utilisé. Les caractéristiques des supports diffèrent selon la nature physique du support et le mode de propagation choisi. Cependant, certaines caractéris-

tiques sont communes à tous les types de support (bande passante...), d'autres sont spécifiques (impédance caractéristique...). Après l'étude générale de ces caractéristiques, nous examinerons et qualifierons chaque type de support.

4.1 CARACTÉRISTIQUES DES SUPPORTS DE TRANSMISSION

4.1.1 Bande passante et système de transmission

Généralités

L'impulsion électrique représentative d'un élément binaire est affaiblie et déformée par le système de transmission (figure 4.2).

Figure 4.2 Déformation du signal par le support de transmission.

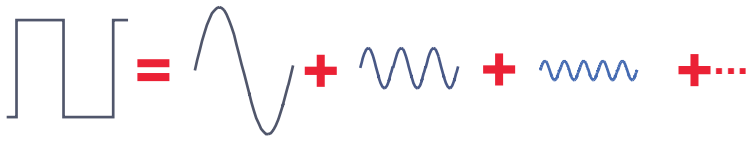
À l'extrémité de la ligne, le récepteur doit identifier et décoder le signal. Cette fonction ne peut valablement être réalisée que si le signal n'a pas été exagérément modifié pendant la transmission. Ces modifications dépendent d'une part de la nature du signal (spectre du signal) et, d'autre part, de la réponse en fréquence du système (bande passante).

Notions d'analyse spectrale

L'impulsion électrique est un phénomène discontinu qui ne peut être modélisé. L'étude du comportement des circuits en régime impulsionnel est essentiellement due aux travaux du mathématicien et physicien Fourier qui a montré que tout signal périodique non sinusoïdal peut être considéré comme la somme d'une composante continue (A_0) et d'une infinité de signaux sinusoïdaux d'amplitude et de phase convenablement choisies. Le théorème de Fourier peut s'exprimer sous la forme de :

$$u(t) = A0 + \sum_{i=1}^{i=\infty} Ui \cos(i\omega t + \varphi i)$$

La composante de même fréquence que le signal d'origine est appelée **fondamental**. Les autres composantes, multiple de la fréquence du signal fondamental, sont appelées **harmoniques**. La figure 4.3 illustre la décomposition d'un signal carré.



$$u(t) = 4\,U / \pi\,(\sin \omega t + 1/3 \sin 3\omega t + 1/5 \sin 5\omega t + \ldots)$$

Figure 4.3 Décomposition d'un signal carré symétrique par rapport au 0 volt.

Un signal périodique quelconque peut donc être considéré comme une infinité de signaux sinusoïdaux. Chaque composante peut être représentée par l'énergie qu'elle contient. Cette représentation est appelée **raie de fréquence** (transformation de l'espace temps en espace fréquence). L'ensemble des raies de fréquence constitue le spectre de fréquences (spectre de raies) du signal. L'espace de fréquence occupé par le spectre se nomme largeur de bande (figure 4.4). En théorie, la largeur de bande d'un signal non sinusoïdal est infinie.

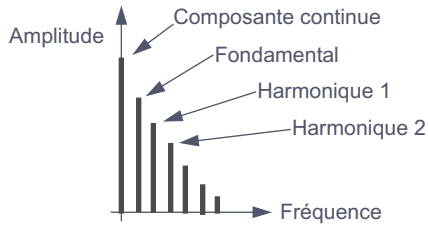


Figure 4.4 Notion de spectre du signal.

La figure 4.5 illustre la reconstitution du signal de la figure 4.3 à partir de ces seules trois premières composantes. En 1, le fondamental et la première composante donne un signal différent du signal d'origine. En 2, on additionne, au signal obtenu en 1, la troisième composante : le signal est plus proche du signal d'origine. En pratique, les cinq premières harmoniques sont suffisantes pour reconstituer un signal satisfaisant.

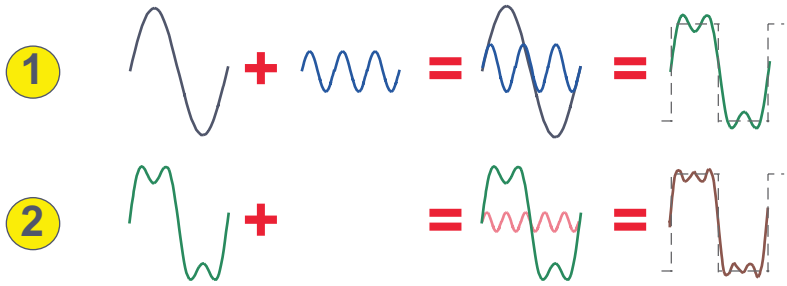


Figure 4.5 Reconstitution du signal d'origine.

Notion de bande passante

Dès lors, pour étudier le comportement d'un système en régime non sinusoïdal on peut étudier celui-ci pour chacune des composantes du signal auquel il sera soumis. La réponse en fréquence de ce système est obtenue en utilisant un générateur dont on fait varier la fréquence à tension constante (générateur de fréquence). La mesure de la puissance en sortie du système permet de tracer une courbe, dite **courbe de réponse en fréquence** (figure 4.6).

La courbe de la figure 4.5 montre que le système de transmission ne transmet pas toutes les composantes de la même manière. Dans ces conditions, le signal en sortie du système n'est plus l'image de celui en entrée, on dit qu'il y a distorsion (figure 4.2). La distorsion est dite en amplitude quand les éléments constitutifs du signal, fondamental et harmoniques, ne sont pas affaiblis identiquement. La distorsion est dite de phase quand les différents éléments du signal ne sont pas tous transmis dans un même délai. Les distorsions d'amplitude et de phase

© Dunod – La photocopie non autorisée est un délit

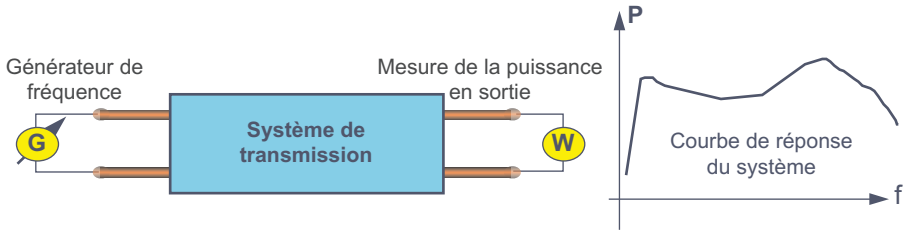


Figure 4.6 Tracé de la bande passante d'un système.

sont généralement indissociables, cependant la distorsion d'amplitude est plus importante que la distorsion de phase.

Les systèmes de transmission (lignes, amplificateurs...) ne transmettent pas toutes les harmoniques du signal de façon identique. Les signaux sont transmis avec une distorsion faible jusqu'à une certaine fréquence appelée **fréquence de coupure**. Au-delà de cette fréquence, toutes les harmoniques sont fortement atténuées. On appelle **bande passante** (figure 4.6) l'espace de fréquences tel que tout signal appartenant à cet intervalle, ne subisse, au plus, qu'un affaiblissement déterminé par rapport à un niveau de référence. L'affaiblissement, exprimé en décibel (dB), est donné par la relation :

$$A = 10 \log_{10} P_1 / P_0$$

P_1 : puissance du signal en sortie P_0 : puissance du signal de référence

La bande passante est généralement définie pour une atténuation en puissance de moitié, ce qui correspond à –3 dB (figure 4.7).

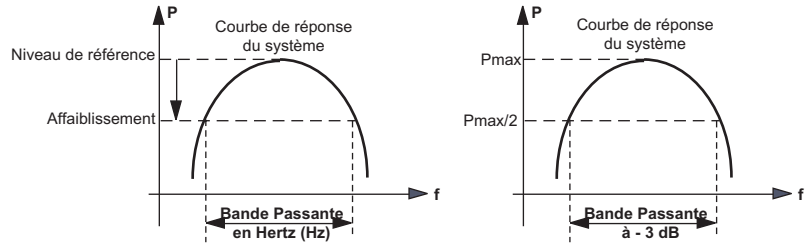


Figure 4.7 Bande passante à –3 dB.

La **largeur de bande** d'un signal correspond à la bande passante minimale que le système doit posséder pour restituer correctement l'information. Ainsi, la bande passante qualifie le système, et la largeur de bande qualifie le signal. Notons que le terme de bande passante est utilisé non seulement pour désigner un espace fréquentiel (Bande Passante ou BP en Hz), mais aussi pour qualifier le débit binaire d'un système (Bande Passante exprimée en bit/s).

Notion de filtre

Un système ne restitue pas les différentes composantes du signal de manière identique, il agit comme un filtre. En fonction de l'espace de fréquence que le système retransmet, on distingue 3 types de filtres (figure 4.8).

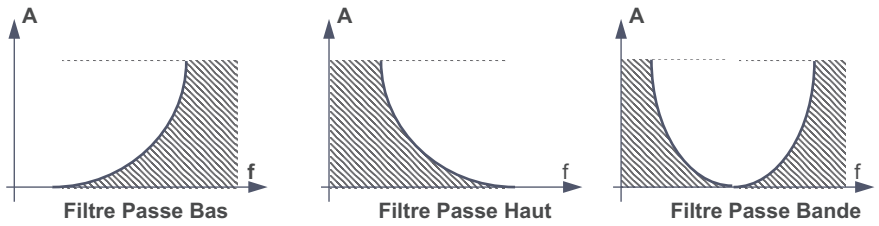


Figure 4.8 Différents types de filtres.

Le filtre passe-bas ne se laisse « traverser » que par les fréquences basses, il atténue les fréquences élevées. À l'inverse, le filtre passe-haut atténue les fréquences basses. En principe un système de transmission se présente à la fois comme un filtre passe-bas et un filtre passe-haut, il laisse passer une certaine bande de fréquence, c'est un filtre passe-bande. Le signal à transmettre devra tenir compte de ces caractéristiques, c'est le rôle rempli par l'ETCD (DCE).

Deux données caractérisent un filtre :

– La fréquence de coupure (fc), ou fréquence à partir de laquelle on considère que toutes les fréquences supérieures et (ou) inférieures sont atténuées d'une valeur donnée (généralement –3 dB).

– La pente de la courbe d'affaiblissement qui s'exprime en dB par octave[1].

4.1.2 Impédance caractéristique

Définition

Une ligne de transmission est constituée de 2 conducteurs de cuivre séparés par un isolant. La figure 4.9 modélise un élément d'une ligne en matérialisant ses composantes physiques. Elle présente au courant électrique un effet résistif (R) responsable de l'atténuation du signal, des effets réactifs qui se décomposent en effet selfique (L) et en effet capacitif (C), et enfin la conductance (G) qui exprime la perte par effet résistif entre les deux conducteurs (généralement négligeable).

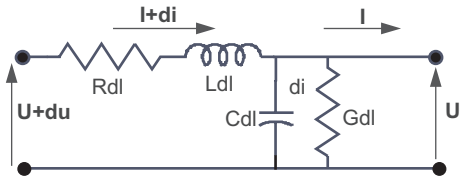


Figure 4.9 Schéma équivalent d'un élément (dl) d'une ligne de transmission.

On appelle impédance (Z) de l'élément de ligne de longueur dl, le rapport du/di. La notion d'impédance en courant alternatif recouvre une notion similaire à celle de résistance en courant continu, elle s'exprime en ohm (Ω). Le rapport du/di pour une ligne supposée de longueur

1. Une octave correspond à une variation de fréquence dans un rapport de 1 à 2.

© Dunod – La photocopie non autorisée est un délit

infinie s'appelle **impédance caractéristique** notée Zc :

$$Zc = \sqrt{\frac{R + jL\omega}{G + jC\omega}} \approx \sqrt{\frac{L}{C}}$$

avec $\omega = 2\pi \cdot f$, ω est la pulsation du courant exprimée en radian/s
f, en Hz, la fréquence du signal

Zc, ou impédance caractéristique, est l'impédance d'une ligne de longueur infinie. On montre (figure 4.10) qu'une ligne de longueur finie refermée sur un récepteur, dont l'impédance Zr est telle que Zr = Zc, se comporte comme une ligne de longueur infinie. Le transfert de puissance est maximum entre le générateur et le récepteur. La ligne est dite adaptée (**adaptation d'impédance**).

Figure 4.10 Notion d'adaptation d'impédance.

Conséquence de la désadaptation d'impédance : l'écho

À chaque rupture d'impédance (Zr # Zc), le transfert de puissance n'est pas optimal, une partie de l'énergie incidente est réfléchie. Cette énergie (onde réfléchie ou **écho**) se combine à l'énergie incidente pour former des ondes stationnaires. En transmission numérique, l'écho a pour conséquence de générer des « bits fantômes », introduisant des erreurs de transmission. La figure 4.11 illustre un système complètement désadapté. A chaque point de raccordement une partie de l'énergie est réfléchie. La source reçoit deux fois le signal d'écho, le premier dû à la rupture d'impédance locale (écho local) est peu gênant. Le second dû à la rupture d'impédance distante (écho distant) est plus gênant, des dispositifs spécifiques (annuleur d'écho) ont en charge de supprimer les effets de cet écho.

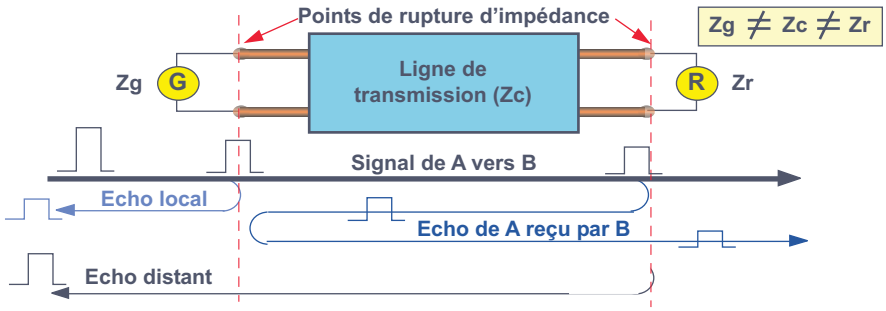


Figure 4.11 Notion d'écho.

Pour éviter ces réflexions parasites, il est nécessaire, tout au long de la ligne et à chaque raccordement d'un nouvel élément à la liaison, de réaliser la continuité de l'impédance : c'est l'adaptation d'impédance. Cependant, celle-ci n'est pas toujours réalisable. Par exemple, la ligne qui raccorde un usager à un réseau peut être en 2 fils, alors que la transmission dans le

réseau de l'opérateur s'effectue en 4 fils (2 fils par sens de transmission), le passage de 2 à 4 fils provoque une rupture d'impédance et des échos. L'emploi d'annuleur d'écho est alors indispensable (figure 4.12).

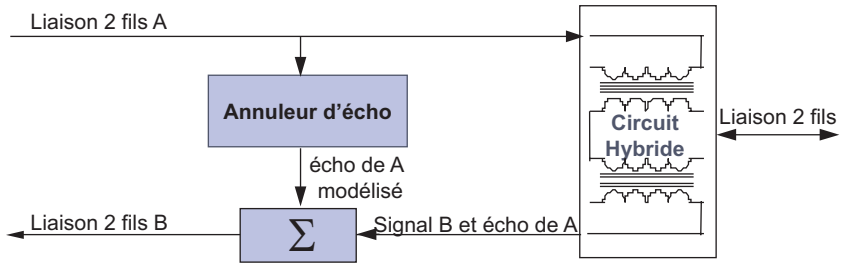


Figure 4.12 Principe de l'annulation d'écho.

Le filtre annuleur d'écho de la figure 4.12 réalise une estimation du signal d'écho en amplitude et phase (modélisation mathématique). Ce signal est ajouté en opposition de phase au signal de l'autre canal. Le système est symétrique pour les deux canaux de communication (injection d'une partie du signal B dans A).

Le *Return Loss* mesure le rapport entre l'énergie transmise et l'énergie réfléchie.

4.1.3 Coefficient de vélocité

Le **coefficient de vélocité** est une grandeur qui mesure la vitesse de propagation du signal dans un support. C'est le rapport entre la vitesse de propagation réelle et la vitesse de la lumière ($c = 3 \cdot 10^8$ m/s). Pour les câbles cuivre, il vaut environ 0,7. Notons que la vitesse de propagation dans un support est une fonction inverse de la racine carrée de la fréquence.

$$V = v.c$$

V : vitesse de propagation réelle du courant en m/s v : coefficient de vélocité
c : célérité ou vitesse de la lumière

Le temps de propagation d'un signal entre sa source et sa destination est fonction de la distance. Ce facteur est peu important quand la transmission a lieu sur un seul support. Dans les systèmes où les données sont transmises simultanément sur plusieurs supports, comme dans le Gigabit Ethernet, les parcours n'étant pas strictement identiques cela pose des problèmes difficiles à résoudre. La différence de temps de propagation (*delay skew*) entre des supports utilisés en parallèle implique l'utilisation de circuits de retard pour réaligner les signaux.

4.2 LES SUPPORTS GUIDÉS

4.2.1 La paire torsadée

Figure 4.13 Paire torsadée ou paire symétrique.

La paire torsadée ou symétrique est constituée de deux conducteurs identiques torsadés. Les torsades réduisent l'inductance de la ligne (L). Généralement plusieurs paires sont regroupées

© Dunod – La photocopie non autorisée est un délit

sous une enveloppe protectrice appelée gaine pour former un câble. Les câbles contiennent 1 paire (desserte téléphonique), 4 paires (réseaux locaux), ou plusieurs dizaines de paires (câble téléphonique).

Caractéristiques

Impédance caractéristique, bande passante et atténuation sont les caractéristiques essentielles des paires torsadées. Cependant, compte tenu de la proximité des différentes paires dans un câble, un phénomène spécifique apparaît : la **diaphonie** (figure 4.14). La diaphonie, due au couplage inductif entre paires voisines, correspond au transfert du signal d'un câble à un autre. Elle limite l'utilisation de la paire symétrique à de faibles distances.

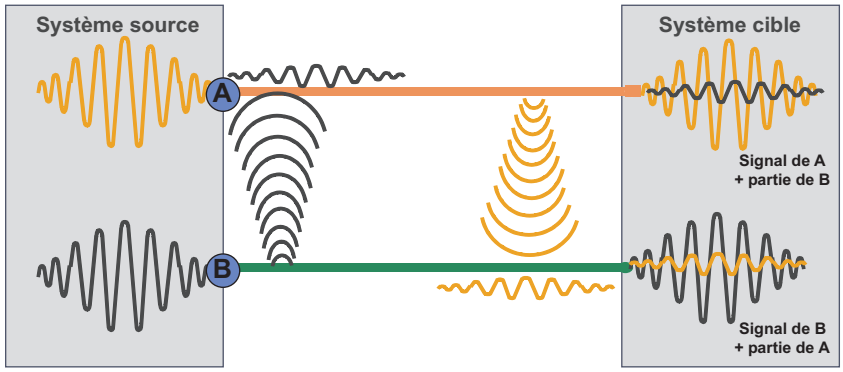


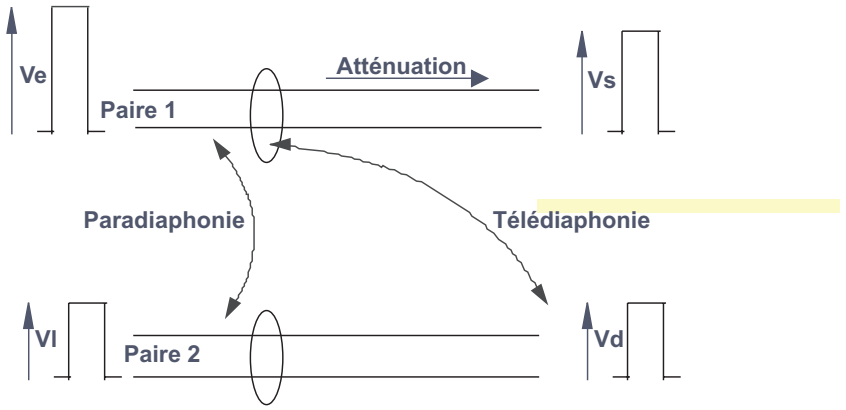
Figure 4.14 Couplage inductif entre paires : la diaphonie.

Deux grandeurs ont été introduites pour mesurer ce phénomène : la paradiaphonie et la télédiaphonie. La paradiaphonie (**Next** ou *Near end crosstalk*) et la télédiaphonie (**Fext** ou *Far end crosstalk*) indiquent l'affaiblissement du signal transmis sur les paires avoisinantes par rapport au signal d'entrée, l'une est mesurée près de la source (*Near*), l'autre à l'extrémité (*Far*). Ces rapports sont exprimés en dB, plus grande est la valeur meilleur est le câble utilisé (figure 4.15).

La paire torsadée (paire symétrique, **UTP** *Unshielded Twisted Pairs*) est sensible à l'environnement électromagnétique (parasites industriels, proximité de câbles à courant fort...). L'utilisation de tels câbles est soumise à des contraintes d'installation. La paire symétrique est généralement utilisée sans référence à la terre (transmission différentielle) ce qui améliore sa résistance aux parasites (voir section 3.3.3).

L'immunité aux parasites peut être améliorée en protégeant le faisceau par un écran (câble écranté). L'écran est constitué d'un ruban d'aluminium qui entoure les paires et les protège des perturbations électromagnétiques. Un conducteur de cuivre nu étamé (drain) permet la mise à la terre de l'écran (paires écrantées, **FTP** *Foiled Twisted Pairs*). Une meilleure protection peut être obtenue en réalisant, autour des paires, un véritable blindage (paires blindées, **STP** *Shielded Twisted Pairs*).

La paire symétrique est actuellement le conducteur le plus utilisé : desserte locale des raccordements téléphoniques, liaisons d'accès aux réseaux de données et surtout les réseaux locaux où les faibles distances autorisent l'utilisation de débits élevés : 100 Mbit/s sur 100 m, voire 1 Gbit/s.



Atténuation A = 20 $\log_{10}$ *Vs* /*Ve* où *Vs* est la tension en sortie
Ve est la tension du signal d'entrée.

Paradiaphonie Next =20 $\log_{10}$ *Vl*/*Ve* où *Vl* est la tension locale induite
Ve est la tension du signal d'entrée.

Télédiaphonie Fext =20 $\log_{10}$ *Vd*/*Ve* où *Vd* est la tension distante induite
Ve est la tension du signal d'entrée.

Figure 4.15 Paradiaphonie et Télédiaphonie.

Les systèmes de précâblage

Le développement intensif des postes de travail connectés, en réseau local ou autre, a révélé des problèmes liés au câblage. Les réseaux locaux ont tous, aujourd'hui, une topologie physique en étoile, d'où l'idée de réaliser, dans les immeubles de bureaux, un précâblage (figure 4.16). Un système de précâblage doit :

– assurer que tout poste de travail ne sera qu'à quelques mètres d'une prise informatique ou téléphonique ;

– être indépendant du type de réseau et de la topologie réseau choisis.

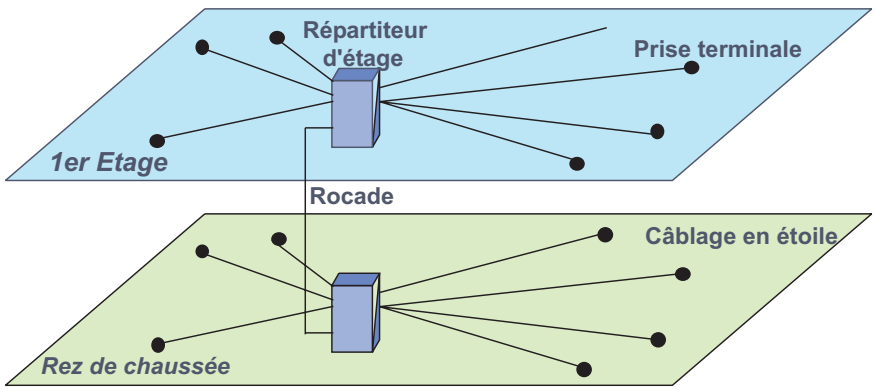


Figure 4.16 Principe d'un précâblage d'immeuble.

© Dunod – La photocopie non autorisée est un délit

Les principaux systèmes sont l'ICS (*IBM Cabling System*), le BCS (*BULL Cabling System*), *l'Open Link* de DEC et le PDS Systimax d'AVAYA. Ces systèmes ont en commun l'utilisation de la paire torsadée et une topologie physique en étoile. Le cœur du câblage est constitué de panneaux, dit **panneaux de brassage**, qui permettent, à l'aide de jarretières, de réaliser la connexion des postes de travail selon la topologie requise par le réseau. Ces systèmes diffèrent essentiellement par le type de câble utilisé (UTP, FTP).

Les câbles ont été répartis en différentes catégories selon les spécifications auxquelles ils répondent (atténuation, bande passante, Next...). Le tableau de la figure 4.17 classe les différents types de câble et indique leur utilisation.

Catégorie	Classe	Bande Passante	Exemples d'utilisation
1 & 2	A, B		Voix (600Ω)
3	C	16 MHz	Voix numérique, réseaux locaux de type Ethernet et Any Lan
4	D	20 MHz	Réseaux locaux de type Token Ring
5	D	100 MHz	Réseaux locaux Ethernet 10 et 100 Mbit/s, Token Ring, Any Lan
6	E	250 MHz	Câble UTP et FTP, Ethernet 1 Gigabit/s
7		600 MHz	Câble FTP

Figure 4.17 Les catégories de paires torsadées.

La catégorie distingue les équipements, la notion de classe de câblage qualifie un câblage de bout en bout. Notons que les câbles 120 Ω catégorie 6 ont été relégués en classe C dans la dernière version de la norme ISO/IEC (IS 11801 du 23 octobre 2002).

4.2.2 Le câble coaxial

Une paire coaxiale ou câble coaxial (figure 4.18) est constituée de deux conducteurs concentriques maintenus à distance constante par un diélectrique. Le conducteur extérieur, tresse métallique en cuivre recuit appelée **blindage**, est mis à la terre. L'ensemble est protégé par une gaine isolante.

Le câble coaxial possède des caractéristiques électriques supérieures à celles de la paire torsadée. Il autorise des débits plus élevés et est peu sensible aux perturbations électromagnétiques extérieures. Le taux d'erreur sur un tel câble est d'environ 10^{-9}.

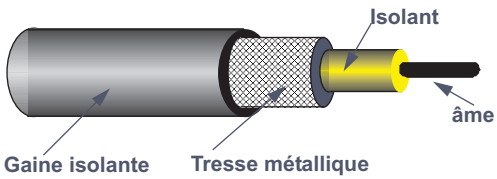


Figure 4.18 Le câble coaxial.

En transmission numérique, notamment dans les réseaux locaux, on utilise des câbles d'impédance 50 Ω à des débits pouvant atteindre 10 Mbit/s sur des distances de l'ordre du kilomètre. En transmission analogique, le câble coaxial est utilisé pour réaliser des liaisons longues distances. Son impédance est de 75 Ω. Ce câble, similaire au câble coaxial utilisé en télévision, est souvent dénommé câble CATV. La bande passante est d'environ 300 à 400 MHz.

Le CATV présente une bonne immunité aux parasites, mais cher et exigeant en contraintes d'installation (rayon de courbure...), il n'est plus utilisé que dans des environnements perturbés ou dans les systèmes sécurisés (rayonnement). Dans les réseaux locaux, il est remplacé par la paire torsadée et dans les liaisons longues distances par la fibre optique.

4.2.3 La fibre optique

Principe

Un faisceau de lumière (figure 4.19), au passage d'un milieu 1 vers un milieu 2 (dioptre), est réfléchi (retour au milieu d'origine) et est réfracté avec une déviation (passage dans le milieu 2). L'indice de réfraction (n_1, n_2) mesure le rapport entre la vitesse de propagation du rayon lumineux dans le vide et celle dans le milieu considéré, soit :

$$n = c/v$$

où n est l'indice de réfraction absolu du milieu considéré, c la vitesse de la lumière dans le vide ($3 \cdot 10^8$ m/s), v la vitesse de propagation de la lumière dans le milieu considéré.

Par exemple, l'indice de réfraction du vide est évidemment de 1, celui du verre ordinaire d'environ 1,5 et de l'eau 1,33.

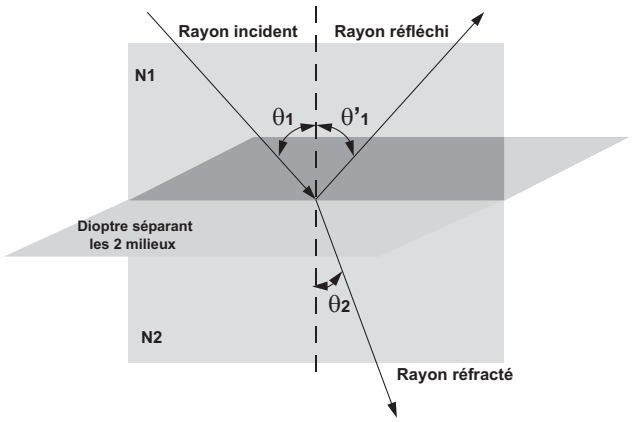


Figure 4.19 La loi de Descartes ($N_1 \sin\theta_1 = N_2 \sin\theta_2$).

Lorsque l'angle d'incidence augmente (θ_1), l'énergie réfractée diminue et l'énergie réfléchie augmente. Si on augmente encore l'angle, la réfraction devient nulle ($\theta_2 = \pi/2$, condition limite de la réfraction) toute l'énergie est réfléchie, la réflexion est totale. Cette propriété est utilisée pour réaliser des guides de lumière : la fibre optique. Une fibre optique (figure 4.20) est composée d'un « fil » de silice appelé **cœur**, entouré d'une gaine appelée **manteau** et d'une enveloppe de protection. La réflexion totale est assurée par des valeurs d'indices proches tel que $n_1 > n_2$ où n_1 est l'indice du cœur et n_2 celui de la gaine.

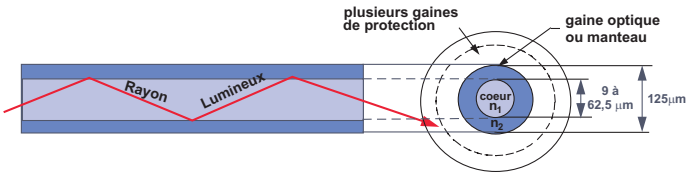


Figure 4.20 La fibre optique : guide de lumière.

© Dunod – La photocopie non autorisée est un délit

Un système de transmission par fibre optique met en œuvre (figure 4.21) :

– un émetteur de lumière (transmetteur), constitué d'une diode électroluminescente (**LED**, *Light Emitting Diode*) ou d'une diode **LASER** (*Light Amplification by Stimulated Emission of Radiation*), qui transforme les impulsions électriques en impulsions lumineuses ;

– un récepteur de lumière, constitué d'une photodiode de type **PIN** (*Positive Intrinsic Négative*) ou de type PDA (à effet d'avalanche) qui traduit les impulsions lumineuses en signaux électriques ;

– une fibre optique.

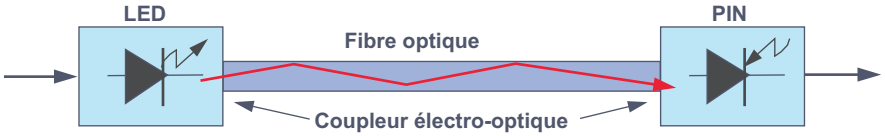


Figure 4.21 Principe d'une liaison optique.

La puissance émise par une LED est peu élevée (≅ 1 mW) et, seul un faible pourcentage de cette puissance est récupéré dans la fibre. Pour les liaisons à haut débit on lui préfère les diodes laser. Ces dernières autorisent une puissance à l'émission voisine de 5 mW avec un rendement de couplage d'environ 50 %. Une LED a une bande passante de 100 MHz, une diode laser permet une largeur de bande de 800 MHz.

La fibre étant un système de transmission unidirectionnel, une liaison optique nécessite l'utilisation de 2 fibres. La figure 4.22 montre la réalisation de coupleurs optiques pour interconnecter deux réseaux locaux.

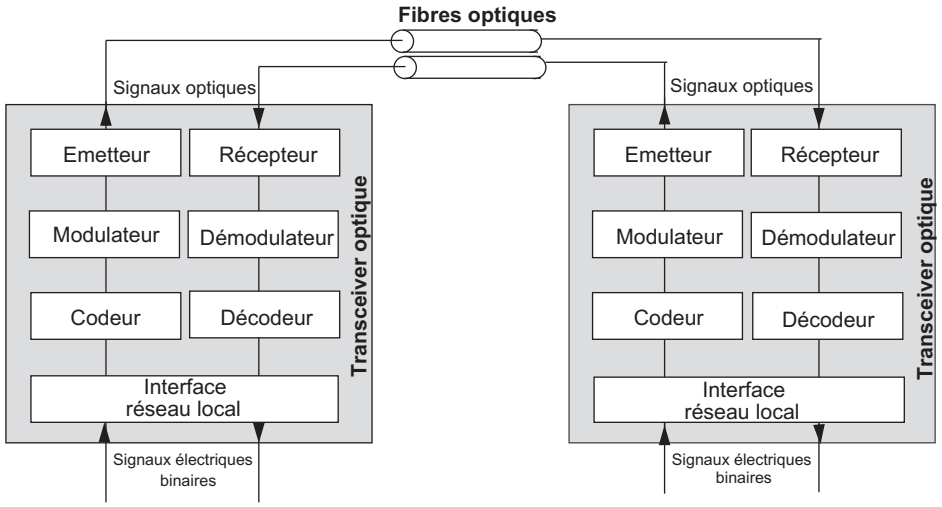


Figure 4.22 Interconnexion de 2 réseaux locaux par fibre optique.

Les différents types de fibres

Les rayons lumineux qui remplissent la condition de réflexion sont acheminés dans le cœur de la fibre. L'ensemble des rayons admis forme un cône, le cône d'acceptance dont l'ouverture ou

angle d'incidence maximal est θ_{max} (figure 4.23). L'ouverture numérique (*ON*) de la fibre est la grandeur qui qualifie le cône d'acceptance ($ON = \sin \theta_{max}$).

➤ Les fibres à saut d'indice

Dans les fibres à saut d'indice, le cœur d'indice n_1 est entouré d'une gaine d'indice n_2. La variation d'indice entre le cœur et la gaine est brutale (saut d'indice). La propagation s'y fait par réflexion totale à l'interface cœur/gaine.

Quand le diamètre du cœur de la fibre est grand devant la longueur d'onde de la lumière, l'ouverture numérique est importante et permet un bon couplage optique. Ce type de fibre autorise l'utilisation de sources de faible puissance (LED). Cependant, la fibre admet plusieurs rayons qui se propagent sur des chemins différents ou modes de propagation. Ces différents trajets provoquent un étalement du signal (dispersion modale ou **DMD**, *Differential Mode Delay*), la fibre est alors dite multimode (**MMF**, *MultiMode optical Fiber*, figure 4.23). La dispersion modale provoque un étalement du signal, ce qui limite la bande passante de la fibre et la distance franchissable.

En réduisant le diamètre du cœur, on réduit l'ouverture numérique. Cette réduction, peut être telle que, pour une longueur d'onde donnée, la fibre n'admette plus qu'un seul rayon. La fibre est alors dite monomode (**SMF**, *Single Mode optical Fiber*), le diamètre du cœur est compris entre 8 et 9 μm et le diamètre du manteau 125 μm. La fibre n'est monomode qu'au-delà d'une certaine longueur d'onde appelée **longueur d'onde de coupure** ($\approx$1 200 nm). La distance franchissable est de l'ordre de 100 km et la bande passante est supérieure à 20 GHz pour une fibre de 1 km. Si la fibre monomode permet de franchir de grandes distances, le couplage optique est faible et demande une source de puissance lumineuse supérieure. La fibre monomode exige l'emploi de diodes laser, d'un coût plus élevé et d'une longévité réduite.

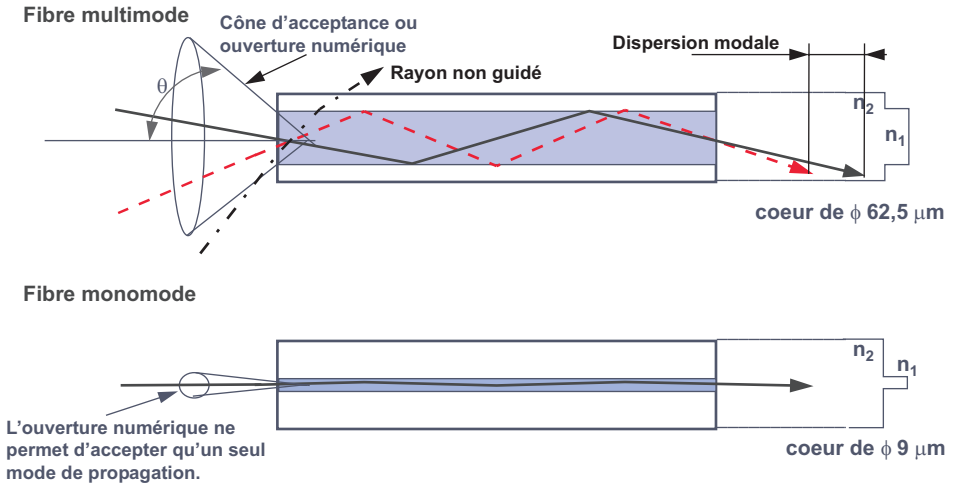


Figure 4.23 Les fibres à saut d'indice.

➤ Les fibres à gradient d'indice

Un compromis a été trouvé avec les fibres à gradient d'indice (figure 4.24), l'indice du cœur décroît de façon continue, depuis le centre du cœur jusqu'à l'interface cœur/gaine suivant une

© Dunod – La photocopie non autorisée est un délit

loi parabolique. Tous les rayons sont focalisés au centre de la fibre, ils ont une trajectoire proche de la sinusoïde. La vitesse de propagation est d'autant plus élevée que l'indice de réfraction est faible. Cette différence de vitesse tend à compenser les différences de trajet, elle réduit la dispersion modale et autorise une portée plus grande que dans les fibres multimodes à saut d'indice. La bande passante, pour une fibre d'un kilomètre est d'environ 500 MHz à 2 GHz et l'affaiblissement de 0,4 dB, ce qui autorise des portées d'environ 50 km.

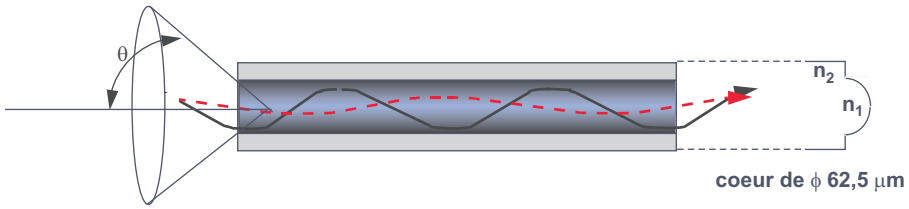


Figure 4.24 Les fibres à gradient d'indice.

Performance des fibres optiques

Dans une fibre optique, on montre que le produit bande passante par la distance est une constante. En général, on exprime la bande passante par km. Compte tenu de la réponse en fréquence des fibres (figure 4.25) et des coupleurs optoélectroniques, on définit trois plages d'utilisation appelées fenêtres optiques proches de l'infrarouge.

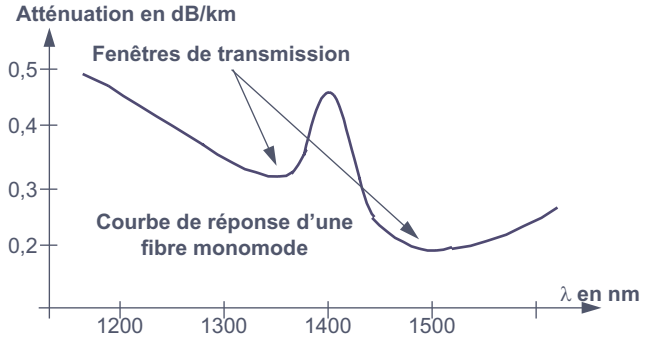


Figure 4.25 Notion de fenêtre optique.

La première fenêtre à 850 nm ($3{,}53 \cdot 10^5$ GHz) correspond à l'utilisation de coupleurs à coût minimal. Ce n'est pas l'optimum d'utilisation des fibres, mais dans des liaisons à faible distance, comme dans les réseaux locaux, cette fenêtre est parfaitement adaptée. Généralement, on lui préfère la fenêtre de 1 300 nm ($2{,}3 \cdot 10^5$ GHz), l'atténuation n'est alors que d'environ 0,5 dB/km. La fenêtre située à 1 550 nm ($1{,}93 \cdot 10^5$ GHz) a l'avantage de ne présenter qu'une atténuation d'environ 0,2 dB/km, mais les coupleurs sont plus coûteux.

Les performances des fibres optiques sont :

– bande passante importante ;
– immunité électromagnétique ;
– faible taux d'erreur 10^{-12} ;

– faible affaiblissement (0,2 à 0,5 dB/km) ;
– faible encombrement et poids ;
– vitesse de propagation élevée (monomode) ;
– sécurité (absence de rayonnement à l'extérieur et difficulté de se mettre à l'écoute) ;
– légèreté.

Ces caractéristiques font des fibres optiques le support privilégié dans le domaine des télécommunications à haut débit et grande distance, dans les applications aéronautiques et navales (sous-marin) et dans les transmissions de données en milieu perturbé.

Si la pose de la fibre optique est aisée (pas de contraintes particulières), la connectique est assez délicate, elle nécessite un outillage particulier et un savoir-faire certain.

4.2.4 Les liaisons hertziennes

Principe

Un conducteur rectiligne alimenté en courant haute fréquence ou radiofréquence peut être assimilé à un circuit oscillant ouvert. Un tel circuit ou antenne d'émission rayonne une énergie (onde électromagnétique). Cette énergie électromagnétique recueillie par un autre conducteur distant ou antenne de réception est transformée en un courant électrique similaire à celui d'excitation de l'antenne d'émission (théorème de réciprocité). La figure 4.26 illustre le principe d'une liaison radioélectrique.

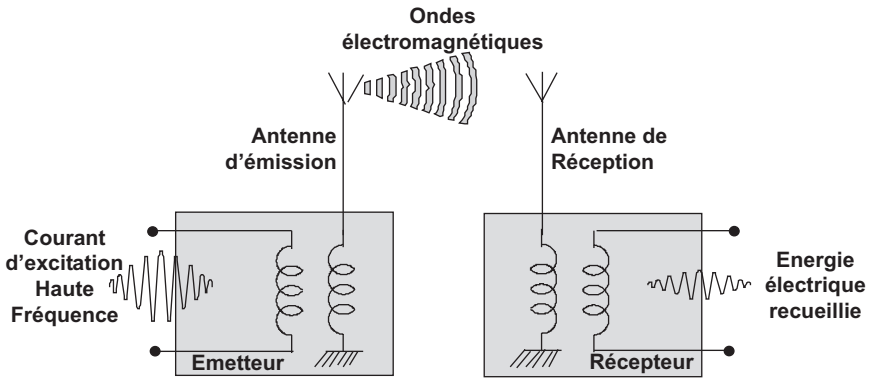


Figure 4.26 Principe d'une liaison radioélectrique.

Contrairement aux supports étudiés dans les paragraphes précédents, la liaison entre les deux entités émetteur et récepteur s'effectue sans support physique. Les ondes électromagnétiques (OEM) se propagent dans le vide à la vitesse de la lumière. On appelle longueur d'onde (λ), la distance parcourue pendant une période du phénomène vibratoire.

Une antenne est un conducteur dont la longueur est un sous-multiple de la longueur d'onde. Le rayonnement d'une source ponctuelle est omnidirectionnel, l'énergie se diffuse selon une sphère. Le rayonnement d'un conducteur rectiligne s'effectue selon un demi-tore. Afin d'utiliser au mieux l'énergie rayonnée, on réalise des réflecteurs. Les réflecteurs peuvent être actifs (rideaux d'antennes) ou passifs (brins, réflecteur plan ou parabolique).

© Dunod – La photocopie non autorisée est un délit

La transmission de données utilise des systèmes passifs à émission directive (téléphonie mobile...), très directive (faisceaux hertziens) ou à diffusion (liaisons satellitaires, mobiles en téléphonie mobile...).

Les ondes électromagnétiques subissent peu d'affaiblissement, leur mise en œuvre est assez aisée et le coût d'infrastructure généralement faible devant les coûts de génie civil engendrés par le passage de câbles physiques. Les transmissions par ondes électromagnétiques sont utilisées chaque fois qu'il est nécessaire :

– de diffuser une même information vers plusieurs utilisateurs (réseaux de diffusion),

– de mettre en relation des stations mobiles (réseaux de messagerie),

– de relier, à haut débit, deux entités éloignées (faisceaux hertziens) ou très éloignées (satellites de communication).

Chaque type de liaison ou d'application utilise des bandes de fréquences différentes. L'espace de fréquences utilisables est limité. La figure 4.27 décrit le spectre de fréquences et positionne le domaine d'utilisation, les ondes radioélectriques s'étendent de quelques dizaines de kHz (ondes longues ou grandes ondes) à plus du THz (ondes quasi optiques). L'usage en est réglementé. Au niveau international, les fréquences sont gérées par l'UIT-TS (Union International des Télécommunications – *Telecommunication Standardization*, ex-CCITT et CCIR). L'attribution locale des fréquences est généralement le fait d'organismes nationaux, en France l'ANF (Agence Nationale des Fréquences) et ART (Autorité de Régulation des Télécommunications).

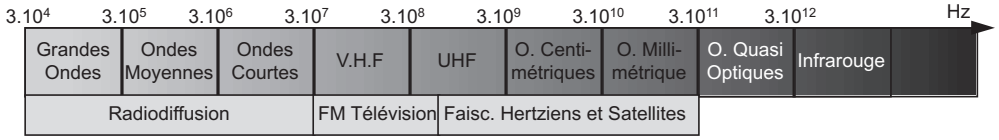


Figure 4.27 Spectre des fréquences.

Les faisceaux hertziens

Les ondes radioélectriques peuvent, dans certains cas, remplacer avantageusement les liaisons filaires (cuivre ou optique). Les faisceaux hertziens ou câbles hertziens, par analogie aux réseaux câblés peuvent être analogiques ou numériques. Les débits peuvent atteindre 155 Mbit/s. Ils sont principalement utilisés pour des réseaux :

– de téléphonie (multiplexage fréquentiel ou temporel),

– de transmission de données,

– de diffusion d'émissions télévisées.

Pour diminuer les puissances d'émission, la technique des faisceaux hertziens utilise des antennes très directives. L'antenne réelle est placée au foyer optique d'une parabole qui réfléchit les ondes en un faisceau d'ondes parallèles très concentré, limitant ainsi la dispersion de l'énergie radioélectrique. En réception, l'antenne est aussi placée au foyer optique de la parabole. Tous les rayons reçus parallèlement à l'axe optique de la parabole sont réfléchis vers le foyer optique, on recueille ainsi, le maximum d'énergie (figure 4.28).

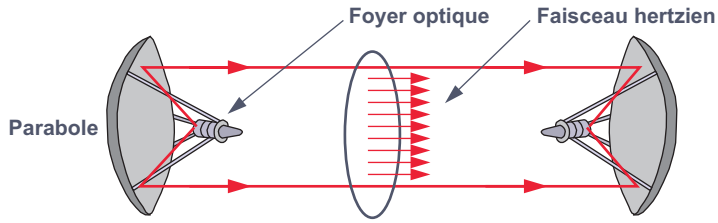


Figure 4.28 Principe des faisceaux hertziens.

Les distances franchissables, par les systèmes de transmission hertzienne, peuvent atteindre 100 km. Pour couvrir des distances plus importantes, il faut disposer des relais. Les relais peuvent être passifs ou actifs. Les relais passifs sont utilisés dans les zones où le relief est important ; il s'agit de simples réflecteurs utilisés pour guider l'onde, par exemple pour suivre une vallée. Les relais actifs nécessitent une infrastructure plus complexe, le signal recueilli est remis en forme, amplifié puis retransmis. Les faisceaux hertziens utilisent les bandes de 2 à 15 GHz et autorisent des débits de 155 Mbit/s.

Les faisceaux hertziens sont sensibles aux perturbations atmosphériques et aux interférences électromagnétiques. Une infrastructure hertzienne repose sur l'existence de canaux de secours qu'ils soient hertziens ou filaires.

Les liaisons infrarouges et lasers constituent un cas particulier des liaisons hertziennes. Elles sont généralement utilisées, pour interconnecter deux réseaux privés, sur de courtes distances, de l'ordre de quelques centaines de mètres.

Les liaisons satellitaires

La nécessité de disposer de stations relais rend difficile la réalisation de liaisons hertziennes à très grande distance, notamment pour les liaisons transocéaniques. C'est pourquoi, dès les années 1960, on s'est orienté vers l'utilisation de satellites relais. Ce n'est qu'avec l'apparition de porteurs capables de satelliser sur des orbites d'environ 36 000 km qu'il a été possible de réaliser des liaisons permanentes avec des satellites fixes par rapport à un observateur terrestre (satellite géostationnaire). Ces satellites ont une période de révolution identique à celle de la terre (23 h 56 min), ils sont dits **géosynchrones**. L'orbite équatoriale est de 42 164 km, soit une altitude exacte au-dessus de la Terre de 35 800 km.

➤ Principe

Une station terrestre émet vers le satellite un flux d'information (voie montante). Le satellite n'est qu'un simple répéteur, il régénère les signaux reçus et les réémet en direction de la Terre (voie descendante). La figure 4.29 illustre le principe d'une liaison satellitaire.

Pour utiliser un satellite comme point nodal d'un réseau terrestre et, non comme simple relais de télécommunication, il est nécessaire d'admettre plusieurs voies montantes. Celles-ci sont alors en compétition pour l'accès au satellite. Plusieurs techniques peuvent être utilisées :

– L'**AMRF** (Accès Multiple à Répartition de Fréquences), consiste à diviser la bande de fréquence du satellite en sous-bandes, chacune réservée à une voie de communication.

– L'**AMRT** (Accès Multiple à Répartition de Temps), la porteuse est commune à tous les

© Dunod – La photocopie non autorisée est un délit

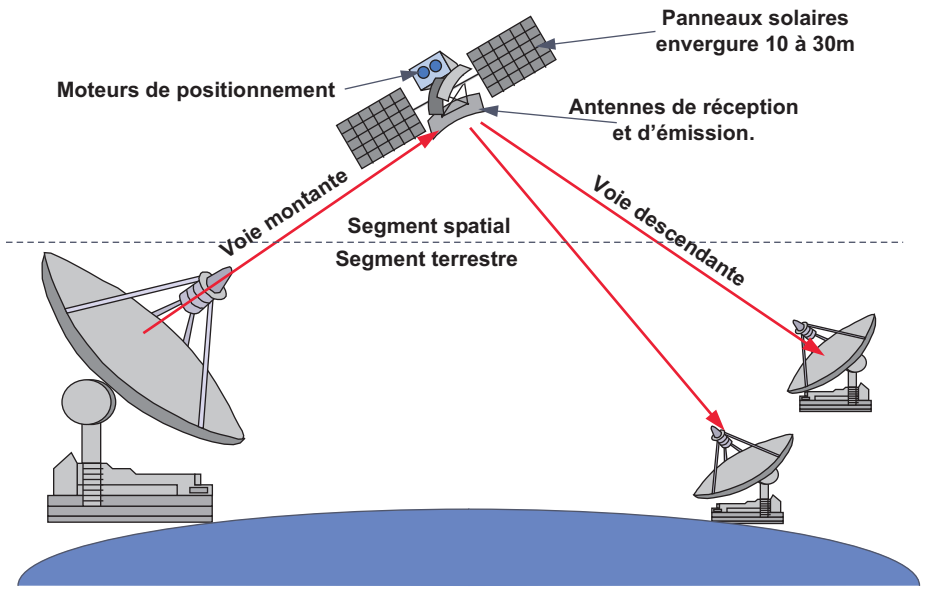


Figure 4.29 Principe d'une liaison satellitaire.

canaux de communication, mais chaque canal n'en dispose que durant un intervalle de temps limité. Ce mode d'accès nécessite une synchronisation entre les stations.

– L'**AMRC** (Accès Multiple à Répartition par Code), dans cette technique on attribue à chaque voie de communication un code. Les informations codées sont envoyées simultanément, elles sont extraites du flux par décodage.

➤ Les différents types de satellites

Compte tenu des temps de propagation des satellites géostationnaires, on a défini plusieurs familles d'orbite. On distingue 3 types de satellites, selon leur orbite : les orbites stationnaires (GEO), moyennes (MEO) et basses (LEO). Le tableau de la figure 4.30 résume les caractéristiques de ces satellites.

La figure 4.31 représente les deux modes orbitales des systèmes de satellites. La partie de droite illustre un système GEO. En orbite équatoriale, avec un cône de rayonnement de 120°, seuls 3 satellites suffisent pour couvrir la Terre, sauf les pôles. Les satellites géostationnaires permettent de réaliser :

– des réseaux de diffusion (radiodiffusion, télévision) ;

– des liaisons point à point ;

– des liaisons à haut débit (bande passante de 500 MHz).

Ces satellites ont un temps de propagation important (environ 240 ms) et un temps de vie limité de 10 à 15 ans par la consommation d'énergie nécessaire à leur maintien sur leur orbite. L'énergie motrice est embarquée, donc limitée, tandis que l'énergie nécessaire au système de télécommunication est fournie par des batteries et panneaux solaires.

La partie de gauche de la figure illustre les systèmes MEO et LEO qui, pour assurer une cou-

	GEO Geostationary Earth Orbit	MEO Medium Earth Orbit	LEO Low Earth Orbit
Altitude	36 000 km	2 000 à 12 000 km	800 à 2 000 km
Type d'orbite	Circulaire	Elliptique ou circulaire	Elliptique ou circulaire
Plan de rotation	Équatorial	Quelconque	Quelconque
Temps de transmission Terre-satellite	240 ms	110 à 150 ms	Environ 50 ms
Permanence spatiale et temporelle (Spatiale : communiquer en tout point Temporelle : en un point à tout moment)	OUI 3 satellites couvrent la terre (sauf les pôles)	NON (orbite défilante) Constellation de satellites	NON (orbite défilante) Constellation de satellites
Applications	Téléphonie fixe, télévision, transmission de données	Téléphonie mobile, transmission de données	Téléphonie mobile, transmission de données
Débit	Jusqu'à 155 Mbit/s	De 9,6 à 38 kbit/s	De 2,4 kbit/s à 155 Mbit/s

Figure 4.30 Synthèse des caractéristiques des différents systèmes de satellites.

verture spatiale et temporelle totale, impliquent l'utilisation d'une constellation de satellites, c'est-à-dire plusieurs orbites et sur chaque orbite plusieurs satellites.

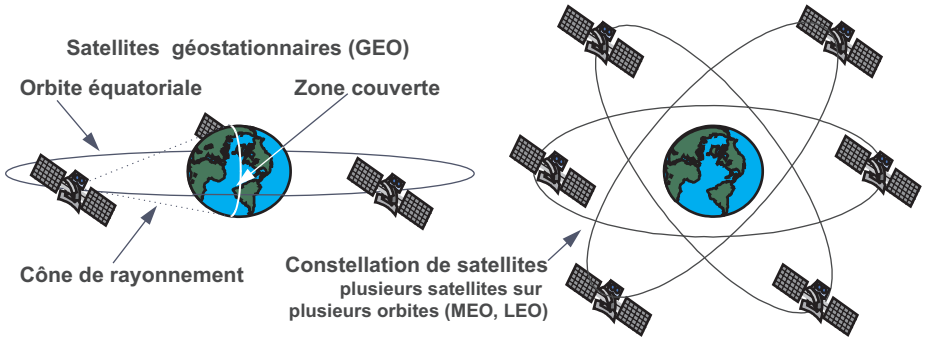


Figure 4.31 Satellites géostationnaires (GEO) et constellation de satellites (MEO et LEO).

4.3 CONCLUSION

Les caractéristiques intrinsèques des supports conditionnent leur limite d'utilisation. Cependant, les progrès importants réalisés par l'électronique numérique reculent de plus en plus ces limites. Les modes de transformation des informations numériques en signal électrique destiné à être acheminé par le support constituent une voie de recherche importante. Ces différents modes de transformation et d'adaptation de l'information au support font l'objet de l'étude du chapitre suivant.

© Dunod – La photocopie non autorisée est un délit

EXERCICES

Exercice 4.1 Notion de décibels

Utilisé dans tous les domaines de la physique, le décibel est une unité logarithmique qui exprime le rapport d'une grandeur (A) par rapport à une autre prise comme référence (B). La relation est de la forme :

$$A/B_{dB} = 10\log_{10}(A/B)$$

Compte tenu de cette définition, quel est le rapport en vraie grandeur des rapports A/B exprimés en dB ?

Valeur en décibel	Rapport en nombre naturel
3 dB	
10 dB	
100 dB	
103 dB	
77 dB	

Exercice 4.2 Portée d'une liaison hertzienne

La propagation des ondes électromagnétiques s'effectue selon plusieurs modes qui dépendent de la fréquence (figure 4.32). Les faisceaux hertziens utilisent la propagation par onde directe ou propagation à vue. Déterminer, en fonction des hauteurs respectives des antennes émission et réception, la portée d'une liaison hertzienne (on supposera la liaison sans obstacle). En déduire la portée théorique des émetteurs de télévision situés au sommet de la tour Eiffel, pour une antenne de réception située à 8 m du sol (cheminée d'une maison basse).

La tour Eiffel et l'antenne distante seront supposées avoir leur assise à la même altitude.

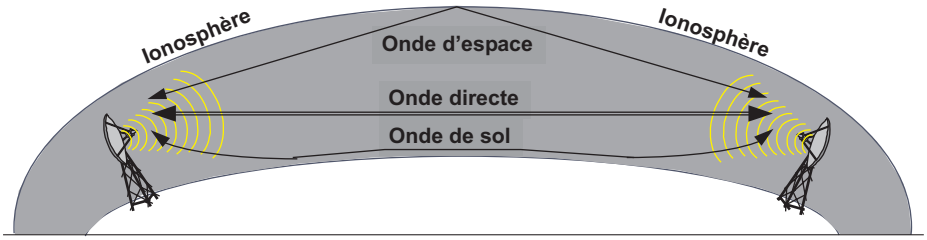


Figure 4.32 Propagation des ondes électromagnétiques (OEM).

L'onde d'espace se propage par réflexion sur la Terre et l'ionosphère. L'onde de sol se propage le long de l'écorce terrestre. L'onde directe se propage à vue en ligne droite (la trajectoire est cependant légèrement incurvée).

Exercice 4.3 Bande passante d'une fibre optique

Une fibre optique multimode à saut d'indice a une ouverture numérique de 0,22 (l'ouverture numérique correspond au sinus de l'angle d'ouverture) et un indice de réfraction du cœur de $n_1 = 1{,}465$. Déterminer la bande passante en bit/s de cette fibre pour une longueur de 1 km (BP/km).

© Dunod – La photocopie non autorisée est un délit

Chapitre **5**

Les techniques de transmission

5.1 GÉNÉRALITÉS

Chaque machine participant à une transmission de données est reliée à la terre locale. Si la terre constitue une référence locale, son potentiel est différent en divers points. De ce fait, réaliser une liaison cuivre directe entre les deux calculateurs provoquerait un courant d'équilibrage qui peut ne pas être supporté par la ligne (intensité) et qui risque de perturber la transmission. Ce problème conduit à distinguer deux références électriques :

– une référence pour la transmission : la terre de signalisation ;

– une référence pour les équipements : la terre de protection.

Cependant, rien ne garantit que dans un équipement les deux terres ne soient pas confondues[1]. Pour pallier ce défaut, on réalise l'isolement galvanique des deux machines par des transformateurs dits *transformateurs d'isolement* (figure 5.1). Ces transformateurs réduisent la bande passante et sont perturbés par la composante continue du signal.

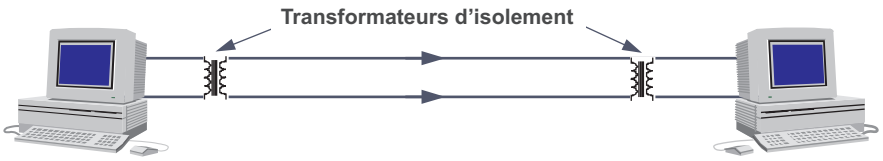


Figure 5.1 Insertion de transformateurs d'isolement sur le lien de transmission.

1. Certaines réglementations nationales imposent la confusion des deux terres.

La ligne de transmission se comporte comme un filtre passe-bas et les transformateurs insérés comme des filtres passe-haut, la ligne de transmission devient alors un filtre passe-bande (figure 5.2).

Figure 5.2 Comportement filtre des éléments de transmission.

Le signal à transmettre devra être adapté au mieux aux contraintes physiques du système de transmission. Deux types d'adaptation ou techniques de transmission sont envisageables (figure 5.3) :

– La première consiste à modifier légèrement le signal, elle est essentiellement destinée à réduire la composante continue. Cependant, les composantes hautes fréquences étant fortement atténuées, la transmission sera limitée en distance : c'est la transmission en bande de base.

– La seconde translate le spectre du signal à émettre dans une bande de fréquences mieux admise par le système, c'est la transmission large bande.

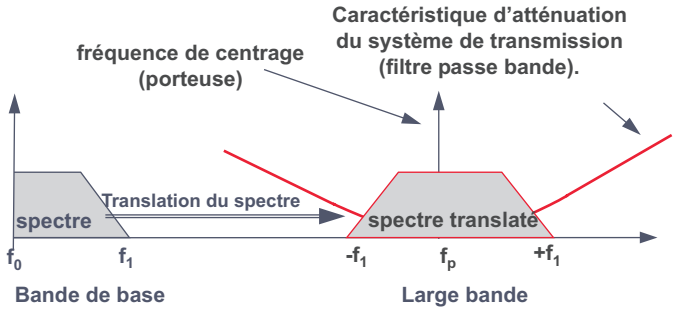


Figure 5.3 Les modes de transmission.

5.2 LA TRANSMISSION EN BANDE DE BASE

5.2.1 Définitions

On qualifie de systèmes de transmission en bande de base les systèmes qui n'introduisent pas d'écart de fréquence entre les signaux émis et ceux reçus. Cette définition n'exclut nullement des modifications du signal pour mieux l'adapter aux caractéristiques du support de transmission.

On appelle **codage**, l'opération qui fait correspondre à un symbole appartenant à un alphabet, une représentation binaire (codage à la source). On désigne par **transcodage**, ou **codage en ligne**, l'opération qui consiste à substituer au signal numérique (représentation binaire) un

signal électrique mieux adapté à la transmission (figure 5.4). Cette transformation est réalisée par un codeur/décodeur appelé Émetteur/Récepteur en Bande de Base (ERBdB).

Figure 5.4 Principe du codage en ligne.

5.2.2 Fonctions d'un codeur/décodeur en bande de base

Le signal numérique, issu du calculateur, présente une composante continue[2] non nulle. Cette composante continue est inutile, elle ne transporte aucune information et provoque un échauffement (effet Joule) des organes d'extrémité (transformateurs d'isolement). Le comportement de filtre passe-bas du système introduit une distorsion de phase qui provoque l'étalement du signal. L'absence de transition, lors de la transmission d'une longue suite de 0 ou de 1, introduit un risque de perte de synchronisation des horloges. Ces différentes considérations conduisent à :

– transformer le signal numérique en un autre, tel que la composante continue soit réduite à son minimum ;
– choisir une méthode de codage pour que le spectre du nouveau signal soit mieux adapté aux caractéristiques du support de transmission ;
– et enfin, pour maintenir la synchronisation, assurer un minimum de transitions, même lors de la transmission de longues séquences de 1 ou de 0.

En résumé, le transcodage, ou codage en ligne, a essentiellement pour objet de supprimer la composante continue, d'adapter le spectre au canal de transmission et de maintenir la synchronisation de l'horloge de réception.

On utilise essentiellement trois types de codes :

– ceux qui effectuent un codage des 1 et 0 (Manchester...) ;
– ceux qui ne codent que les 1 ou les 0 (bipolaire...) ;
– ceux qui substituent à un ensemble de n bits un autre ensemble de m bits (nBmB).

5.2.3 Les principaux codes utilisés

En symétrisant le signal par rapport au potentiel de référence (0 volt), on diminue la composante continue. Pour cela, on représente les 1 (ou les 0) par une valeur + V et les 0 (ou les 1) par – V. Ce codage élémentaire connu sous le nom de code **NRZ** (*No Return to Zero*, non-retour à zéro) est à la base de tous les codes (figure 5.5). Cependant, le spectre de ce signal est relativement large. Il présente un maximum de puissance à la fréquence zéro, ce qui correspond à une composante continue importante.

2. La composante continue représente la valeur moyenne du signal pour un intervalle de temps donné.

© Dunod – La photocopie non autorisée est un délit

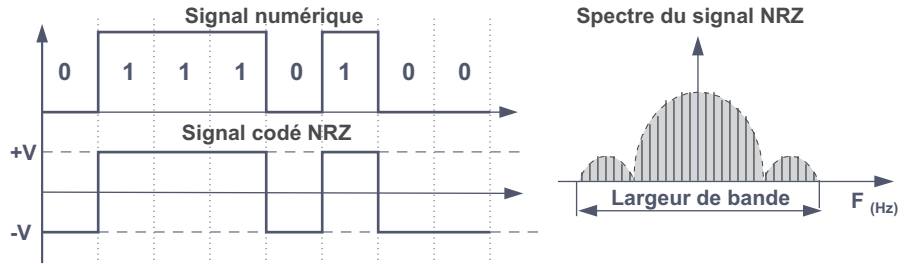


Figure 5.5 Le signal NRZ.

Le codage NRZ symétrise la valeur 1 et la valeur 0 par rapport à un niveau potentiel nul. Cependant ce codage a une composante continue non nulle et ne présente aucune transition lors de longues séquences de 0 ou de 1.

Avec une transition au milieu de chaque temps bit, le codage Manchester (figure 5.6) remédie à l'absence d'information de synchronisation. La transition est croissante pour les 0, décroissante pour les 1. Le sens des transitions est significatif, ce qui pose des problèmes en cas d'inversion des fils de liaison. Multipliant les transitions, le codage Manchester a un spectre très large, il est utilisé dans les réseaux locaux de type Ethernet sur câble coaxial. La bande passante du support y est importante et gratuite et l'inversion de fils impossible.

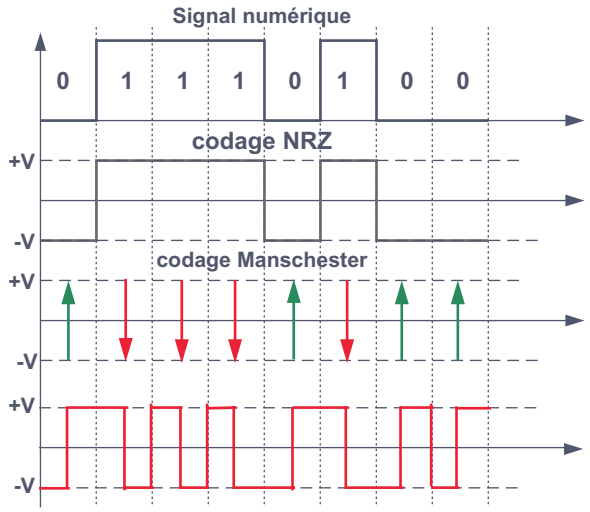


Figure 5.6 Construction du code Manchester.

Le codage Manchester différentiel (figure 5.7) résout le problème d'inversion des conducteurs. Chaque transition, au milieu du temps bit, est codée par rapport à la précédente. Si le bit à coder vaut zéro la transition est de même sens que la précédente ($\Delta\varphi = 0$), si le bit est à 1 on inverse le sens de la transition par rapport à celui de la précédente ($\Delta\varphi = \pi$). Ce codage résout la plupart des problèmes posés, mais son spectre est relativement large. Il est utilisé dans les réseaux locaux de type Token Ring.

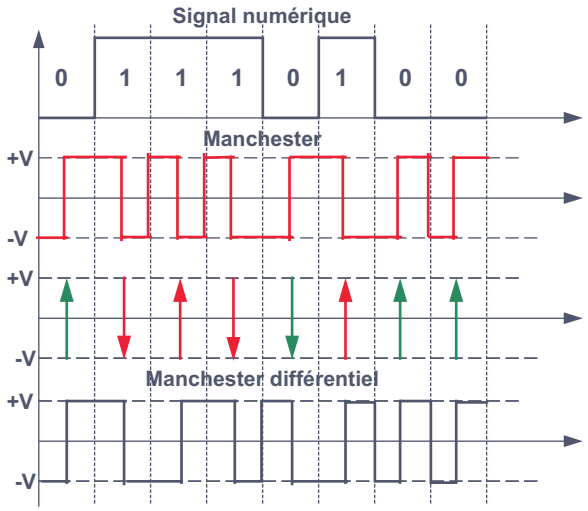


Figure 5.7 Code Manchester différentiel.

Pour réduire le spectre on peut, à partir du Manchester simple, supprimer une transition sur deux, que celle-ci soit ou non significative, on obtient alors le code dit *Delay Mode* ou Miller (figure 5.8). En appliquant cette règle, on constate que les 1 ont une transition au milieu du temps bit et les 0 pas de transition. Mais un 0 suivi d'un 0 a une transition en fin du temps bit.

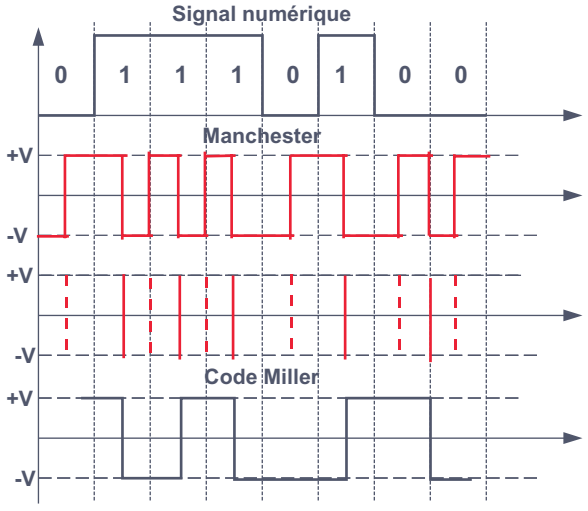


Figure 5.8 Code de Miller.

Une réduction encore plus significative du spectre peut être obtenue en ne codant qu'un type de bit (par exemple les 1) et en alternant leur polarité pour éliminer la composante continue (figure 5.9). Cependant, lors de longues séquences de 0, ou de 1, il n'y a pas de transition (risque de perte de l'horloge) ce code est appelé *code bipolaire*.

© Dunod – La photocopie non autorisée est un délit

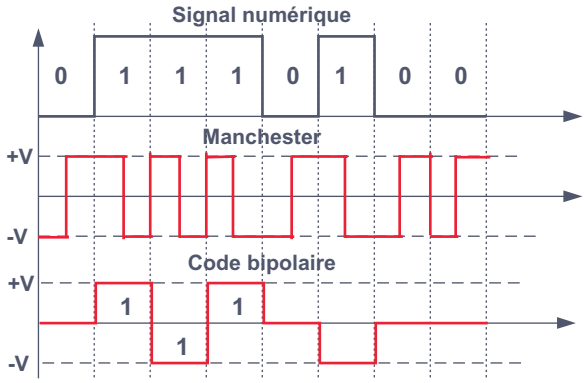


Figure 5.9 Principe des codes bipolaires.

Pour éviter de longues séquences sans transition (suite de 0), les codes **HDBn** (Haute Densité Binaire d'ordre n) sont des codes bipolaires dans lesquels, si le bit de rang n + 1 est à zéro, on le remplace par un bit particulier. Ce bit, sans signification numérique (bit électrique), viole la loi d'alternance des bits (**bit de viol**). Ce viol de polarité permet de le distinguer des bits significatifs. Pour respecter la loi d'alternance du codage (composante continue à zéro), les bits de viol doivent alternativement être inversés (comme les bits à 1). De ce fait, les bits de viol peuvent ne plus être en viol par rapport au dernier bit à 1. Dans ce cas, pour éviter la confusion, on introduit un bit supplémentaire, dit **bit de bourrage**, qui rétablit le viol. Ainsi, en HDB3, les séquences de 4 bits à zéro successifs peuvent être codées : B00V ou 000V (V signifiant Viol et B Bourrage). HDB3 est utilisé dans les liaisons spécialisées louées[3], une représentation en est donnée figure 5.10.

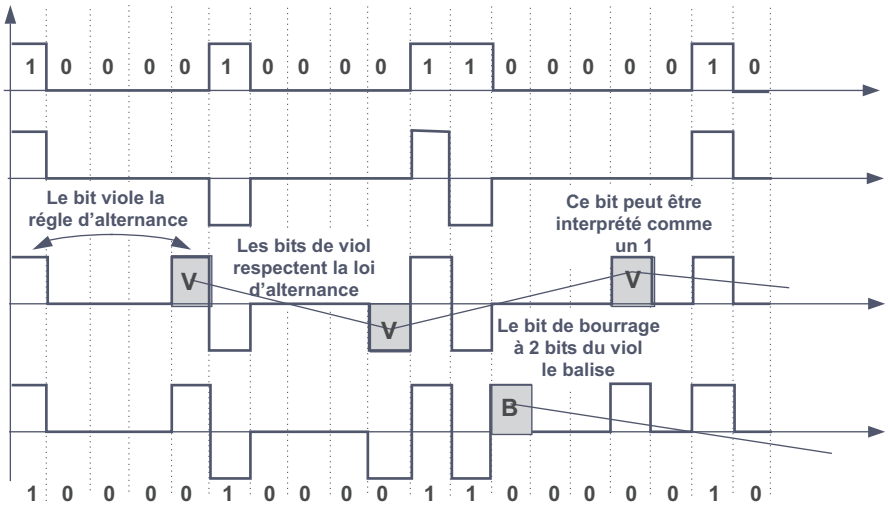

1 0 0 0 0 1 0 0 0 0 1 1 0 0 0 0 0 1 0
Le bit viole la régle d'alternance
Les bits de viol respectent la loi d'alternance
Ce bit peut être interprété comme un 1
V
V
V
Le bit de bourrage à 2 bits du viol le balise
B
1 0 0 0 0 1 0 0 0 0 1 1 0 0 0 0 0 1 0

Figure 5.10 Le code HDB3.

3. Les liaisons louées sont des liaisons misent à disposition d'une personne privée par un opérateur public moyennant une redevance d'usage. France Telecom offre ce service sous le nom de Transfix.

La troisième catégorie de code, dit nBmB avec m > n, est utilisée dans les réseaux à hauts débits. Dans ces codes, on substitue à une combinaison binaire de n bits une autre combinaison de m bits. Le principe de tels codes est représenté figure 5.11.

Figure 5.11 Principe du codage nBmB.

Le choix de 2^n valeurs parmi 2^m permet de résoudre facilement les problèmes de composante continue, de largeur de spectre et parfois autorisent une autocorrection. Les combinaisons binaires sont choisies de telle manière qu'au moins une transition soit assurée pendant un intervalle de temps t dépendant essentiellement de la stabilité de l'horloge de réception.

Dans le code 4B5B, une séquence de 4 bits binaires est remplacée par une combinaison de 5 bits. Les séquences de 5 bits, ou **symboles**, sont choisies de telle manière qu'aucune ne commence par plus d'1 bit à 0 et qu'aucune ne se termine par plus de 2 bits à 0. Ainsi, ce code garantit qu'aucune séquence de plus de 3 bits consécutifs à 0 ne sera transmise. Le tableau de la figure 5.12 indique les codes valides. Les réseaux de type Ethernet à 100 Mbit/s et **FDDI**[4] utilisent le codage 4B5B. Certaines combinaisons, non représentées, sont utilisées pour représenter les commandes de contrôle du réseau FDDI.

Symbole	Valeur binaire	code 4B/5B	Symbole	Valeur binaire	code 4B/5B
0	0000	11110	8	1000	10010
1	0001	01001	9	1001	10011
2	0010	10100	A	1010	10110
3	0011	10101	B	1011	10111
4	0100	01010	C	1100	11010
5	0101	01011	B	1101	11011
6	0110	01110	E	1110	11100
7	0111	01111	F	1111	11101

Figure 5.12 Codage 4B5B de FDDI.

La montée en débit des réseaux locaux sur paires torsadées conduit à rechercher des schémas de codage de plus en plus efficaces, mais de plus en plus complexes.

5.2.4 Le codeur bande de base ou émetteur récepteur en bande de base

Le signal transcodé n'a aucune signification binaire, ce n'est que la représentation électrique du signal numérique. C'est par abus de langage qu'on appelle ce signal « signal numérique », on devrait plutôt parler de signal impulsionnel. L'opération d'adaptation au support (transcodage ou codage en ligne) est effectuée les **ERBdB** (Émetteur Récepteur en Bande de Base, figure 5.13) souvent improprement appelés modems bande de base.

4. FDDI, *Fiber Distributed Data Interface*, réseau local à haut débit voir chapitre 13, *Les réseaux métropolitains*.

© Dunod – La photocopie non autorisée est un délit

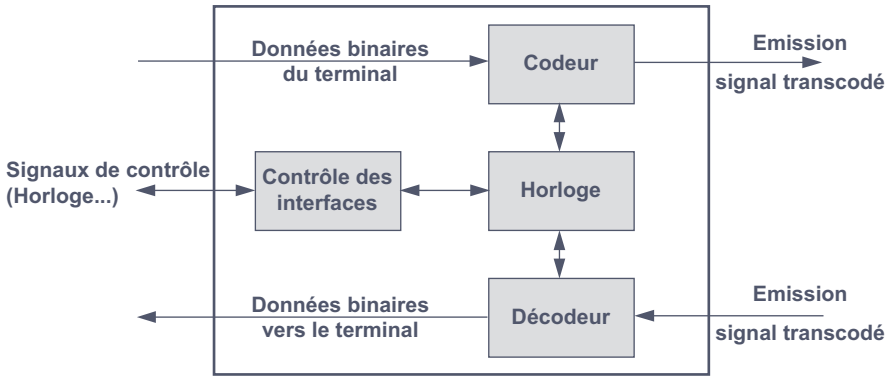


Figure 5.13 Schéma synoptique simplifié d'un Émetteur Récepteur en Bande de Base.

5.2.5 Limitations de la transmission en bande de base

La transmission en bande de base est une technique simple à mettre en œuvre, mais elle est limitée par la bande passante du canal de communication et par le rapport signal sur bruit de celui-ci.

Critère de Nyquist

➤ Notions de rapidité de modulation

Une ligne ou canal de transmission se comporte comme un filtre passe-bas, les différentes composantes sont atténuées (distorsion d'amplitude) et retardées (distorsion de phase). L'une des conséquences les plus visibles est l'étalement du signal. Dans des conditions limites, cet étalement a pour conséquence que la fin d'une impulsion transmise se confond avec le début de la suivante. Les circuits électroniques ne peuvent, alors, distinguer deux impulsions successives, il y a interférence de symboles (figure 5.14).

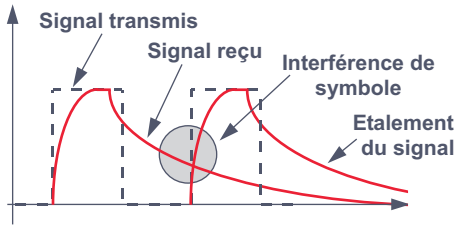


Figure 5.14 L'étalement du signal ne permet plus la récupération d'horloge.

Il existe une relation étroite entre le nombre maximal de symboles (impulsions électriques) que le système peut admettre et la bande passante de celui-ci. Supposons un signal de fréquence F, deux instants significatifs peuvent être distingués. Le premier correspond à la première alternance du signal, le second à la seconde. En assimilant chaque alternance à une impulsion électrique, le nombre maximal d'impulsions que peut transmettre un système, par unité de temps, est, au plus égal au nombre d'alternances du signal (alternance positive pour un « 1 », alternance négative pour le « 0 », par exemple). Soit R_{max}, le nombre maximal de temps

élémentaires par unité de temps (nombre d'impulsions), et F_{max}, la fréquence de coupure du système, ils sont liés par la relation :

$$R_{max} = 2 \cdot F_{max}$$

Si on assimile F_{max} à la bande passante (BP) du canal, on obtient la relation[5] appelée **critère de Nyquist** :

$$R_{max} \leqslant 2 \cdot BP$$

où R_{max} désigne le nombre maximal de transitions qu'un système peut supporter, et est appelé **rapidité de modulation**. La rapidité de modulation, grandeur analogue à une fréquence, s'exprime en baud et représente le nombre d'instants élémentaires du signal par unité de temps. La rapidité de modulation est aussi appelée vitesse de signalisation sur le support.

➤ Application au canal téléphonique

Quelle est la rapidité de modulation maximale admissible sur une voie téléphonique caractérisée par une bande passante (BP) allant de 300 à 3 400 hertz ?

La bande passante a pour valeur :

$$BP = 3\,400 - 300 = 3\,100 \text{ Hz}$$

La rapidité de modulation maximale est :

$$R_{max} = 2 \cdot BP = 2 \cdot 3\,100 = 6\,200 \text{ bauds.}$$

Si durant un intervalle de temps significatif le symbole ne peut prendre que les valeurs 0 ou 1, le débit binaire du canal est égal à la rapidité de modulation. Pour la ligne RTC (Réseau Téléphonique Commuté) de l'exemple ci-dessus, le débit binaire ne peut excéder 6 200 bit/s.

Rapidité de modulation et débit binaire

Imaginons que, durant un temps élémentaire, le symbole prenne plusieurs états (figure 5.15), la quantité d'information transportée alors par un symbole est supérieure à 1 bit. Débit binaire et rapidité de modulation sont liés par la relation :

$$D = R \cdot Q = R \cdot \log_2(1/p)$$

D : débit binaire exprimé en bit/s — R : rapidité de modulation en baud
Q : quantité d'information en bit ou Shannon — p : probabilité d'apparition d'un état

Si on appelle valence du signal (v) le nombre d'états que peut prendre le signal durant un temps élémentaire (v = 1/p). Le débit s'exprime, alors, par la relation :

$$D = R \cdot \log_2 v = 2 \cdot BP \cdot \log_2 v$$

avec D le débit binaire en bit/s, v la valence du signal, valant 1/p, et R la rapidité de modulation.

5. La relation trouvée est très théorique. En effet, Nyquist a considéré le système comme étant un filtre passe-bande idéal (fréquences de coupure nettes).

© Dunod – La photocopie non autorisée est un délit

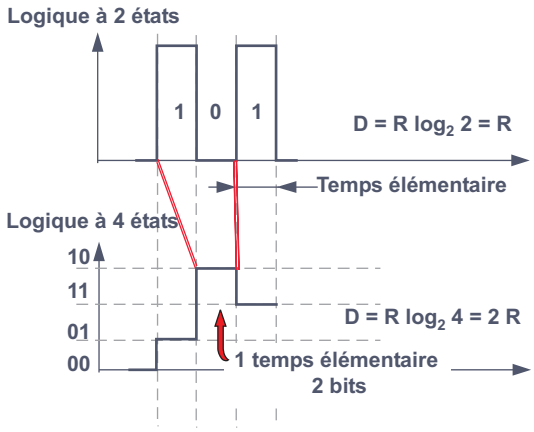


Figure 5.15 Notion de valence du signal.

Dans le cas de l'exemple précédent (voir section 5.2.5.1), la rapidité de modulation est égale au débit binaire. Si durant le temps élémentaire, le signal peut prendre plusieurs valeurs, par exemple 4 (figure 5.15), la probabilité d'apparition d'une valeur est de 0,25. Dans ces conditions, le débit du canal est :

$$D = R \cdot \log_2(1/0,25) = R \cdot \log_2 4 = 2 \cdot R \text{ bit/s}$$

Le débit binaire est le double de la rapidité de modulation. C'est ainsi qu'il est possible d'augmenter, sur un canal de transmission de bande passante limitée, le débit binaire.

L'opération qui consiste à faire correspondre à un ensemble de symboles binaires (00, 01... 000, 001...) un ensemble de valeurs représentatives d'une combinaison binaire (amplitude, fréquence ou phase), durant un intervalle de temps élémentaire, est effectuée par un codeur.

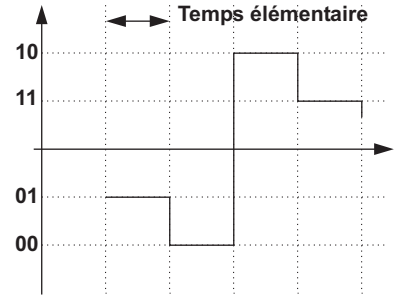


Figure 5.16 Codage 2B1Q.

Le schéma de la figure 5.16 code la suite binaire 01001011 soit 8 bits en 4 temps d'horloge. Ce type de codage, utilisé sur les liaisons RNIS, est dénommé 2B1Q (2 bits, 1 symbole quaternaire soit 1 temps d'horloge, 4 valeurs). En conclusion, rappelons que l'on peut augmenter les possibilités de débit binaire, sur un canal de transmission donné, en agissant sur :

– la bande passante du canal ;

– et/ou la valence du signal transporté.

La bande passante est limitée par le système de transmission (support...) et on ne peut augmenter indéfiniment le nombre d'états du signal (valence), car les niveaux d'amplitude à discriminer deviennent si faibles qu'ils ne peuvent être distingués du bruit (figure 5.17).

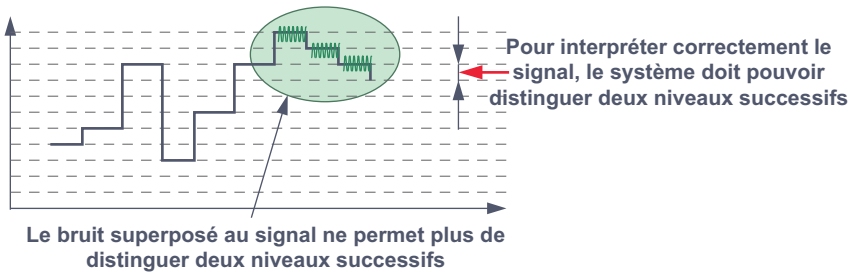

Pour interpréter correctement le signal, le système doit pouvoir distinguer deux niveaux successifs
Le bruit superposé au signal ne permet plus de distinguer deux niveaux successifs

Figure 5.17 Limitation du nombre d'états par le bruit.

Transmission en milieu bruyant

➤ Notion de bruit

Les signaux transmis sur un canal peuvent être perturbés par des phénomènes électriques ou électromagnétiques désignés sous le terme générique de **bruit**. On distingue essentiellement deux types de bruit : le **bruit blanc** et le **bruit impulsionnel**.

Le bruit blanc provient de l'agitation thermique des électrons. Ses composantes (raies de fréquence) sont également réparties dans le spectre des fréquences, d'où son nom. D'amplitude généralement faible, il est peu gênant pour les transmissions.

Le bruit impulsionnel est une perturbation brève qui a pour origine l'environnement physique du canal de transmission (parasite d'origine électromagnétique). D'intensité élevée et d'apparition erratique, il provoque des erreurs portant sur un ensemble de bits.

Rappelons que, le rapport entre la puissance du signal transmis et celle du signal de bruit ou rapport signal sur bruit (S/N avec N pour *Noise*), s'exprime en dB et vaut :

$$S/N_{\text{dB}} = 10 \log_{10} S/N_{(\text{en valeur})}$$

➤ Capacité d'un canal perturbé, relation de Shannon

Reprenant les travaux de Nyquist, Claude Shannon a montré, qu'en milieu perturbé, le nombre maximal d'états discernables ou **valence** est donné par la relation :

$$n = \sqrt{1 + \frac{S}{N}}$$

La capacité maximale de transmission d'un canal est alors de :

$$C = 2 \cdot BP \cdot \log_2 n = BP \cdot \log_2[1 + (S/N)]$$

➤ Application au RTC

Quelle est la capacité maximale de transmission sur une voie RTC caractérisée par une bande passante de 300/3 400 Hz et un rapport signal sur bruit de 1 000 ?

© Dunod – La photocopie non autorisée est un délit

La rapidité de modulation maximale de ce canal est :

$$R_{\max} = 2 \cdot BP = 2(3\,400 - 300) = 6\,200\text{bauds}$$

La capacité de transmission est donnée par la relation de Shannon :

$$\begin{aligned} C &= BP \cdot \log_2[1 + (S/N)] \\ &= (3\,400 - 300)\log_2(1 + 1\,000) \approx 3\,100 \cdot 3,32\log_{10}(1\,000) \\ &= 3\,100 \cdot 3,32 \cdot 3 \\ &= 30\,876\ \text{bit/s} \end{aligned}$$

Ce débit maximal théorique correspond aux performances maximales que l'on peut obtenir sur une ligne téléphonique[6].

➤ Conclusion

La bande passante ou encore la rapidité de modulation et le rapport signal sur bruit limitent les possibilités de transmission en bande de base. La transmission bande de base occupe la totalité de la bande passante du canal interdisant l'utilisation des techniques de multiplexage (voir chapitre 7, *Mutualisation des ressources*).

Les techniques dites « bande de base » restent utilisées sur des liaisons spécialisées privées, les liaisons louées par les opérateurs aux entreprises pour se constituer des réseaux privés, les liaisons d'accès aux réseaux des opérateurs et les réseaux locaux d'entreprise. En l'absence de normalisation concernant les ERBdB, il est impératif d'associer ces équipements par paire de même référence chez un même constructeur. Les ERBdB couvrent une gamme de débits allant de 2 400 bit/s à 2 Mbit/s. La distance maximale d'utilisation dépend essentiellement de la qualité du support utilisé et du débit en ligne, elle varie de quelques kilomètres à quelques dizaines de kilomètres.

5.3 LA TRANSMISSION EN LARGE BANDE

5.3.1 Principe

Transmission bande de base et large bande

En transmission large bande, le spectre du signal numérique est translaté autour d'une fréquence centrale appelée **porteuse**. La translation de spectre résout les deux problèmes posés par la transmission en bande de base : dispersion du spectre (étalement du signal) et la monopolisation du support qui interdit le multiplexage. Elle est réalisée par un organe appelé modulateur. En réception le signal doit subir une transformation inverse, il est démodulé. Le modem, contraction de **mod**ulation/**dém**odulation, est un équipement qui réalise la modulation des signaux en émission et leur démodulation en réception.

6. Le débit maximal sur ligne téléphonique ordinaire (BP = 300 – 3 400 Hz) est aujourd'hui atteint par les modems V34 bis (33 600 bit/s).

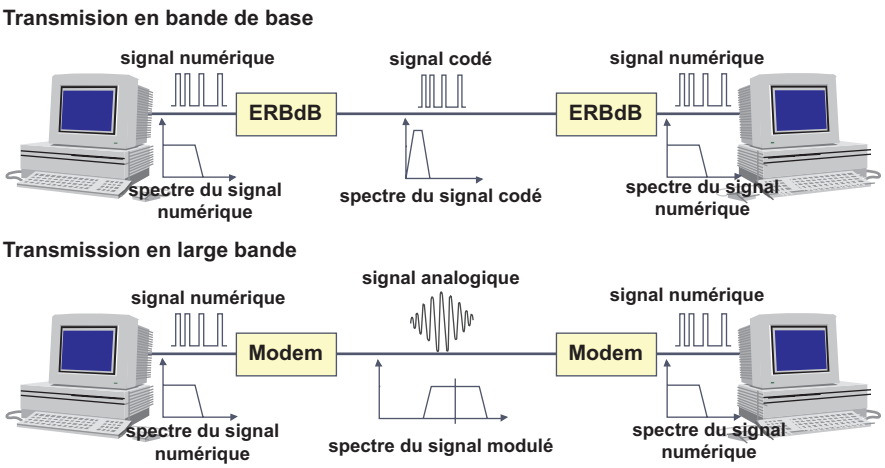


Figure 5.18 Comparaison des modes de transmission.

La figure 5.18 compare les signaux et les spectres respectifs des deux modes de transmission. Il convient ici de préciser des termes dont l'emploi est généralement ambigu. Seul le signal entre le calculateur (ETTD) et l'ETCD ou DCE (codeur ou modem) est un signal numérique. Le signal en ligne est une représentation de celui-ci soit par simple codage (bande de base) soit après modulation (large bande). Dans ce dernier cas, et seulement dans celui-ci, le signal en ligne est qualifié d'analogique.

Principe de la modulation

La dégradation du signal impulsionnel de la bande de base est rapide, la distance franchissable est limitée à quelques km. Le signal sinusoïdal est plus résistant, d'où l'idée de substituer au signal impulsionnel, un signal sinusoïdal et de modifier l'un de ses paramètres en fonction du signal numérique d'origine : c'est la **modulation**. Un signal sinusoïdal est de la forme :

$$u = A_0 \sin(\omega_0 t + \varphi_0) \quad \text{avec} \quad \omega_0 = 2\pi f_0$$

Sur un tel signal, on peut faire varier :

- l'amplitude A_0, c'est la modulation d'amplitude (**ASK**, *Amplitude Shift Keying*) ;
- la fréquence f_0, c'est la modulation de fréquence (**FSK,** *Frequency Shift Keying*) ;
- la phase φ_0, c'est la modulation de phase (**PSK,** *Phase Shift Keying*).

➤ La modulation d'amplitude

La modulation d'amplitude établit une correspondance entre l'amplitude d'un signal sinusoïdal et la valeur d'un signal numérique. Les variations d'amplitude du signal modulé sont alors l'image du signal modulant. Pour retrouver le signal d'origine (signal numérique), il suffit d'interpréter l'enveloppe du signal modulé (amplitude). C'est la démodulation (figure 5.19).

Soit S_0, le signal source ou signal à transmettre, supposé sinusoïdal de fréquence f_0, son spectre est représenté par une seule raie, et P_p le signal modulant ou **porteuse** supposé lui aussi sinusoïdal.

© Dunod – La photocopie non autorisée est un délit

Soit S_m le signal en sortie du modulateur, il comprend une partie de la porteuse (modulation d'amplitude avec porteuse) et un signal égal au produit du signal modulant et de la porteuse, ce signal est de la forme :

$$s_m(t) = kp_p(t) + s_0(t) \cdot p_p(t)$$

où $s_o = S_o \cos(\omega_o t)$ est le signal modulant, $p_p = P_p \cos \omega_p t$ est le signal porteur et k est un coefficient dépendant du système

$$s_m(t) = kP_p \cos \omega_p t + P_p S_0(\cos \omega_p t \cdot \cos \omega_0 t)$$

En posant $k P_p = A_p$ et $P_p S_0 = 2 M_0$ on écrit :

$$s_m = A_p \cos \omega_p t + 2M_0(\cos \omega_p t \cdot \cos \omega_0 t)$$

Ce qui peut s'écrire en développant :

$$s_m = A_p \cos \omega_p t + M_0 \cos(\omega_p - \omega_0)t + M_0 \cos(\omega_p + \omega_0)t$$

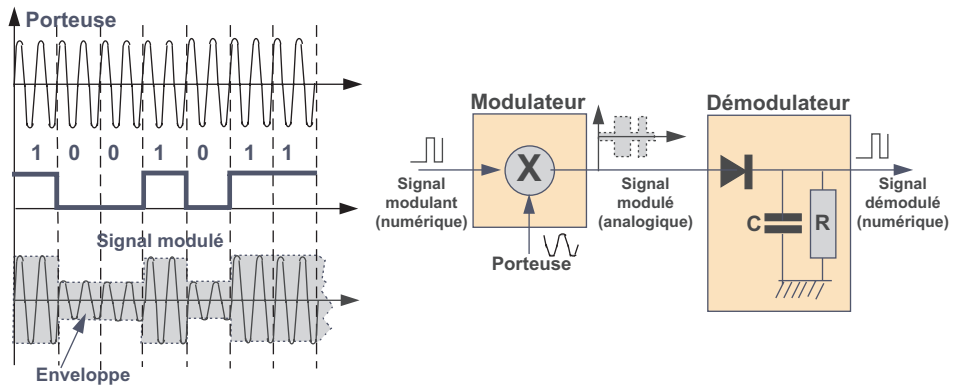


Figure 5.19 Principe de la modulation d'amplitude.

Le signal résultant comporte 3 raies de fréquence, le signal porteur ou porteuse (A_p) à la fréquence f_p et le signal modulé (M_0) avec ses deux raies l'une à $f_p - f_0$ et l'autre à $f_p + f_0$. Remarquons qu'après modulation, l'espace de fréquences utilisé est le double de celui du signal modulant mais centré autour du signal porteur, c'est la transposition de fréquence (figure 5.20).

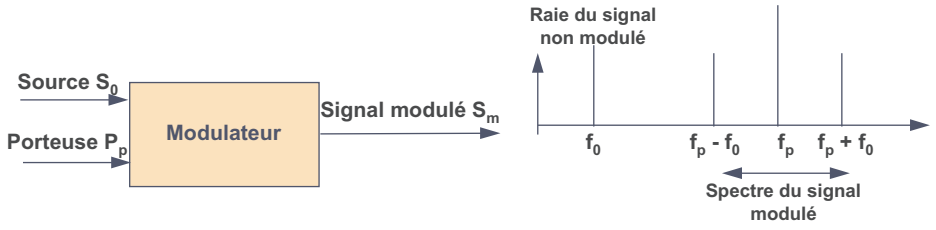


Figure 5.20 Spectre du signal modulé en amplitude.

D'une manière générale, le spectre transposé d'un signal de largeur de bande $[f_1, f_2]$ avec $f_2 > f_1$, s'étend de $f_p - f_2$ à $f_p + f_2$, centré autour de f_p, fréquence du signal translateur ou

porteuse. Chaque demi-spectre ou bande latérale contient l'intégralité de l'information à transmettre. Aussi, pour réduire la largeur de bande et la dispersion du spectre, certains équipements n'utilisent qu'une seule des deux bandes latérales (**BLU**, Bande Latérale Unique). La porteuse, nécessaire à la démodulation, est régénérée par le récepteur.

L'amplitude étant représentative de l'information, la modulation d'amplitude est très sensible aux bruits parasites, elle n'est pratiquement utilisée qu'en combinaison avec la modulation de phase.

➤ La modulation de fréquence

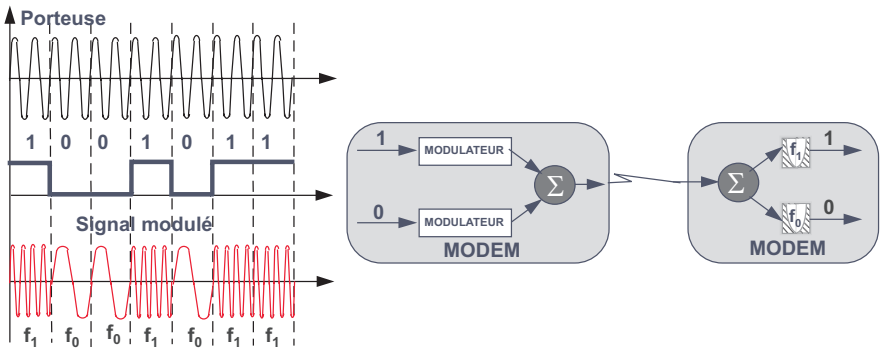


Figure 5.21 Principe de la modulation de fréquence.

Dans ce type de modulation, on associe à une valeur binaire (0,1, ou 01,10...) une fréquence particulière (figure 5.21). En réception, un filtre permet la restitution de la valeur binaire d'origine. La technique de la modulation de fréquence est particulièrement simple à mettre en œuvre. Elle est très résistante aux bruits, mais la grande largeur du spectre du signal résultant la limite au faible débit comme pour le modem V.23 utilisé par le Minitel.

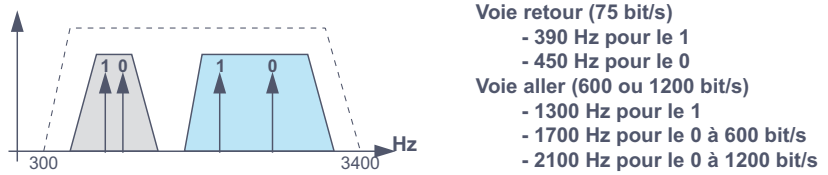

1 0
1 0
Hz
300
3400
Voie retour (75 bit/s)
- 390 Hz pour le 1
- 450 Hz pour le 0
Voie aller (600 ou 1200 bit/s)
- 1300 Hz pour le 1
- 1700 Hz pour le 0 à 600 bit/s
- 2100 Hz pour le 0 à 1200 bit/s

Figure 5.22 Spectre du modem V.23.

Le modem V.23 est conçu pour fonctionner sur ligne téléphonique ordinaire (Bande Passante 300-3 400 Hz). Il permet de réaliser des liaisons *full duplex* asymétriques (la voie aller et la voie retour ont des débits différents). La figure 5.22 indique les fréquences affectées à chaque valeur binaire.

➤ La modulation de phase

En modulation de phase, on associe une valeur binaire à un signal dont la phase est fixée par rapport à un signal de référence. Dans la figure 5.23, la valeur binaire 1 est associée à un signal en phase avec le signal de référence, et la valeur binaire 0 à un signal déphasé de 180°. La représentation est bivalente : modulation de phase à deux états ou **BPSK**, *Binary Phase Shift Keying*.

© Dunod – La photocopie non autorisée est un délit

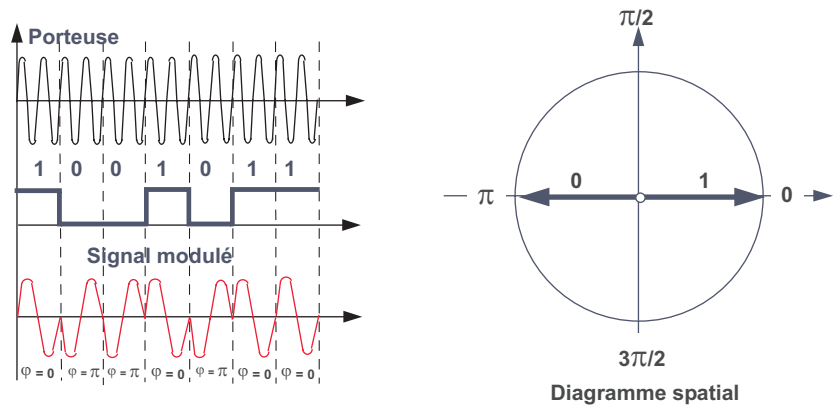


Figure 5.23 Principe de la modulation de phase.

Si le procédé est simple en émission, il est plus complexe en réception. En effet, il faut reconstituer une porteuse de référence avec une probabilité non nulle d'inversion de phase, donc d'inversion du décodage. Pour cela, dans ces systèmes, une séquence d'initialisation précède l'envoi de données.

On peut facilement multiplier les états représentés. Pour une représentation quadrivalente, il est possible d'associer les déphasages φ_n et les valeurs binaires telles que :

$$\begin{aligned} 00 &\Rightarrow \varphi_1 = 0° \\ 01 &\Rightarrow \varphi_2 = \pi/2 \\ 10 &\Rightarrow \varphi_3 = \pi \\ 11 &\Rightarrow \varphi_4 = 3\pi/2 \end{aligned}$$

Cette technique est limitée par l'erreur de phase introduite par le bruit (figure 5.24). On peut aussi combiner la modulation de phase et la modulation d'amplitude, on obtient des schémas de modulation complexes mais très efficaces. Ce type de modulation appelé modulation en amplitude à porteuse en quadrature (**MAQ**, ou **QAM** *Quadrature Amplitude Modulation*) ou en treillis résiste bien au bruit et autorise des débits élevés avec une rapidité de modulation relativement faible.

La figure 5.24 représente le diagramme spatial d'un schéma de modulation à 16 états (MAQ16). Remarquons que les niveaux d'amplitude significatifs de deux vecteurs voisins sont différents. Ce type de codage rend possible, en réception, l'estimation du symbole le plus vraisemblable et améliore la résistance aux erreurs.

Les modems de la dernière génération peuvent mettre en œuvre des codages jusqu'à 64 états, autorisant ainsi des débits élevés avec une rapidité de modulation faible. Par exemple, la modulation MAQ32 définit une modulation à 32 états. Pour un débit effectif de 9 600 bit/s la rapidité de modulation n'est que de :

$$D = R \log_2(1/p)$$

où p, la probabilité de réalisation de l'information, vaut p = 1/32.

Soit, compte tenu que $\log_2 32 = 5$ (pour mémoire $2^5 = 32$)

$$R = D/\log_2 32 = 9\,600/5 = 1\,920 \text{ bauds.}$$

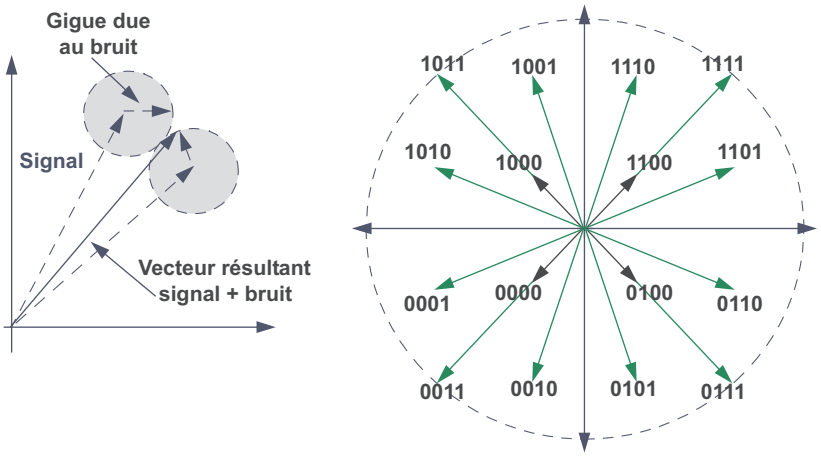


Figure 5.24 Principe de la modulation MAQ (MAQ16) et ses limitations.

5.3.2 Les liaisons full duplex

Les liaisons *full duplex* (figure 5.25) peuvent être réalisées simplement par l'utilisation de 2 voies de communications distinctes (liaisons 4 fils) ou par mise en œuvre de techniques spécifiques (liaison 2 fils).

Figure 5.25 Liaisons *full duplex* à 4 et 2 fils.

En transmission large bande, il est facile de réaliser une liaison full duplex sur deux fils par simple décalage des porteuses comme, par exemple dans le modem V.23 (figure 5.22). En transmission bande de base, cette technique est inapplicable. L'émetteur et le récepteur sont raccordés à la liaison 2 fils par un système hybride permettant le passage de 4 en 2 fils, ce système n'isole pas parfaitement les deux voies. Une partie du signal d'émission se retrouve sur la voie de réception (écho local et écho distant). Le système annuleur d'écho évalue la valeur de ces signaux parasites et les ajoute en opposition de phase au signal reçu. La figure 5.26 illustre ce système.

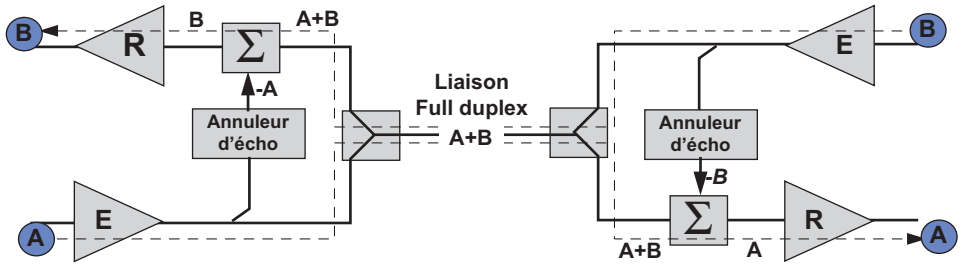


Figure 5.26 Système hybride de passage de 4 à 2 fils.

Les systèmes à annulation d'écho sont aussi utilisés dans les modems large bande.

© Dunod – La photocopie non autorisée est un délit

5.3.3 Dispositifs complémentaires

Les dispositifs d'embrouillage

Les dispositifs d'embrouillage ont pour rôle de modifier les données pour équi-répartir la distribution des 0 et des 1. Cette méthode de modification des données à transmettre facilite la récupération du rythme d'horloge. Dans les ETCD *full duplex* à annulation d'écho, les techniques d'embrouillage facilitent le discernement des deux voies.

L'embrouillage consiste à assimiler les données à transmettre aux coefficients d'un polynôme (D_x), à diviser celui-ci par une séquence pseudo-aléatoire (d_x), enfin à transmettre le quotient (Q_x) et le reste (R_x) de cette division [7]. Le récepteur ayant connaissance du diviseur retrouve les données (le dividende D_x) en effectuant l'opération (débrouillage) :

$$D_x = Q_x \cdot d_x + R_x$$

Le brouillage en émission et le débrouillage en réception sont réalisés par des registres à décalage de n étages comportant une ou plusieurs portes OU exclusifs (figure 5.27).

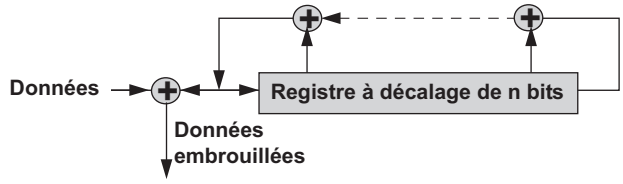


Figure 5.27 Principe d'un embrouilleur.

L'avis V.22 (modem V.22) mettent en œuvre un circuit embrouilleur/débrouilleur utilisant le polynôme :

$$d_x = 1 + x^{14} + x^{17}$$

L'avis V.32 et V.32 bis utilisent deux polynômes :

– dans le sens appel (celui qui initialise la liaison) $x^{23} + x^{18} + 1$

– dans le sens réponse $x^{23} + x^5 + 1$.

La compression de données et le mode correction d'erreurs

Le constructeur américain Microcom, en dotant ses modems de fonctions évoluées (détection et correction d'erreurs, compression...), a créé un standard. Les fonctions offertes par les modems Microcom (figure 5.28) sont connues sous le nom de *Microcom Networking Protocol* (**MNP**). Certaines de ces fonctions ont fait l'objet de normalisation. L'avis V.42 pour le contrôle d'erreur entre modems a pour origine MNP 4, alors que l'avis V.42bis pour la compression de données est issu des protocoles MNP2, 3 et 4.

Les fonctionnalités MNP sont de moins en moins supportées par les modems des dernières générations. Cependant pour assurer la compatibilité, certains constructeurs intègrent les fonctions équivalentes normalisées et les fonctions MNP d'origine.

7. La technique de la division polynômiale, utilisée aussi pour la détection des erreurs de transmission, sera étudiée au chapitre 7.

MNP 1	Protocole de correction d'erreurs au niveau de l'octet, il n'est plus utilisé aujourd'hui.
MNP 2	Protocole de correction d'erreurs au niveau de l'octet en full duplex, pour liaison asynchrone en full duplex à 2 400 bit/s.
MNP 3	Protocole de correction d'erreurs au niveau bit, il utilise le protocole SDLC en full duplex. Mis en œuvre dans les liaisons asynchrones (vu des ETTD, le protocole de transmission est asynchrone alors que les modems, ou ETCD, conversent en mode synchrone).
MNP 4	Protocole de correction d'erreurs au niveau paquet. La taille des paquets est variable (*Adaptative Packet Assembly*) en fonction de la qualité de la ligne ; utilisé pour des liaisons asynchrones sur le RTC.
MNP 5	Protocole de correction d'erreurs et de compression de données (combinaison du code d'Huffman et du *Run Length Encoding*). Le taux de compression peut atteindre 2.
MNP 6	Semblable à MNP5, MNP 6 simule une liaison *full duplex* sur une liaison *half duplex*, en mettant en œuvre un procédé de retournement de modem très rapide.
MNP 7	Amélioration du protocole MNP 5 en associant la compression d'Huffman à un algorithme de prédiction, le taux de compression peut atteindre 3.
MNP 8	N'est plus commercialisé.
MNP 9	Protocole de correction d'erreurs et de compression de données pour modems asynchrones ou synchrones à 38,4 kbit/s, ou 9 600 sur liaison RTC.
MNP 10	Amélioration de MNP 4, MNP 10 autorise l'adaptation dynamique de la taille des paquets et un repli de la vitesse de transmission.

Figure 5.28 Synthèse des protocoles MNP.

Le langage de commande

Hayes, autre constructeur américain de modems (*Hayes Microcomputer Products*), est connu par l'implémentation dans ses modems d'un langage de commande qui est devenu un véritable standard.

Le langage Hayes ne nécessite pas l'utilisation d'un logiciel spécifique pour piloter le modem, c'est l'une des raisons de son succès.

Tant que le modem n'est pas connecté à un équipement distant, il considère que ce qu'il reçoit est une commande et il l'exécute. Lorsqu'il est connecté, il est transparent aux caractères reçus : ce qu'il reçoit, il le transmet. Le langage Hayes, implémenté par de nombreux constructeurs, dans leurs équipements, n'est pas normalisé. Le respect plus ou moins rigide du standard Hayes crée des incompatibilités entre modems, et entre modems et logiciels. Le CCITT (UIT-T) a spécifié un langage de commande pour modem dérivé du langage Hayes.

Les commandes Hayes (figure 5.29) commencent toutes par les deux lettres AT (attention) suivies d'une lettre qui indique la commande et, éventuellement, de paramètres. La commande ATD 01 46 35 53 99 signifie « composer le numéro 01 46 35 53 99 ».

Tests de fonctionnement

Lors d'incidents de fonctionnement, il peut être intéressant de localiser l'élément défectueux par simple bouclage des composants sans avoir à se déplacer. La recommandation V.54 du CCITT (UIT-T) définit quatre bouclages (figure 5.30) qui sont :

© Dunod – La photocopie non autorisée est un délit

– le bouclage 1, pontage entre le terminal et le modem (l'ETTD et ETCD), permet de tester le fonctionnement de l'ETTD ;
– le bouclage 2, effectué entre l'ETCD et ETTD récepteurs, vérifie l'intégrité de la liaison, modems y compris ;
– le modem local peut être vérifié par le bouclage 3 ;
– le bouclage 4 autorise l'évaluation de la qualité de la liaison (réservé aux lignes à 4 fils).

Commandes	Signification	Commentaires
+++	Séquence d'échappement	Permet de revenir en mode commande en cours de communication.
ATA	Answer	Prise de ligne immédiate en réponse.
ATD	Dial	Numérotation automatique, la commande est suivie du numéro et éventuellement de caractères : - T, numérotation en fréquence. - P, numérotation par impulsion. - R, appel en mode retourné. - , (virgule) pause de 2 secondes. - ; (point virgule) retour en mode commande après numérotation.
ATE	Echo	Paramétrage de l'écho des commandes : - ATE 0, pas d'écho. - ATE 1, écho des commandes.
ATF	Full	Choix entre half ou full duplex : - ATF 0, half duplex. - ATF 1, full duplex.
ATH	Hang	Raccrocher.
ATM	Monitor	Paramétrage du haut parleur : - ATM 0, pas de haut-parleur. - ATM 1, haut-parleur jusqu'à la connexion. - ATM 2, haut-parleur permanent.
ATO	On Line	Prise de ligne immédiate (correction manuelle).
ATQ	Quiet	Paramétrage des messages : - ATQ 0, émission de messages de comptes rendus (OK, ERROR...). - ATQ 1, la carte n'émet aucun message.
ATS		Lecture et écriture des registres : - ATS x ?, lecture/affichage du contenu du registre x. - ATS x = nn, écriture de nn dans le registre x.
ATV	Verbal	Sélection du type de messages émis par la carte. - ATV 0, message numérique. - ATV 1, message en clair.
ATX		Extension de message : - ATX 0, message normal. - ATX 1, message étendu
ATZ		Réinitialisation de la carte.

Figure 5.29 Les commandes Hayes.

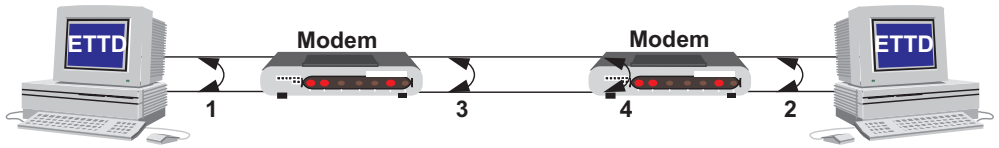


Figure 5.30 Le bouclage des modems.

Les indicateurs de fonctionnement

Les modems sont généralement dotés d'indicateurs d'état qui permettent d'en contrôler le fonctionnement. Ces indicateurs numérotés selon une convention que nous étudierons un peu plus tard (voir figure 5.40) sont :

– Ali témoin d'alimentation du modem.
– 103 visualise l'émission de données.
– 104 indique une réception de données.
– 106 le modem est prêt à émettre.
– 109 le modem reçoit une porteuse (liaison avec un modem distant établie).
– 142 le modem est en cours de bouclage.

5.3.4 Exemples de modem

Synoptique d'un modem

Le synoptique du modem représenté figure 5.31 correspond à celui d'un modem synchrone. En fonctionnement asynchrone, les circuits débrouillage et horloge interne ne sont pas en fonction.

Un modem comprend deux parties, l'émetteur de données ou modulateur et le récepteur de données ou démodulateur. Les fonctions remplies par chaque partie sont symétriques.

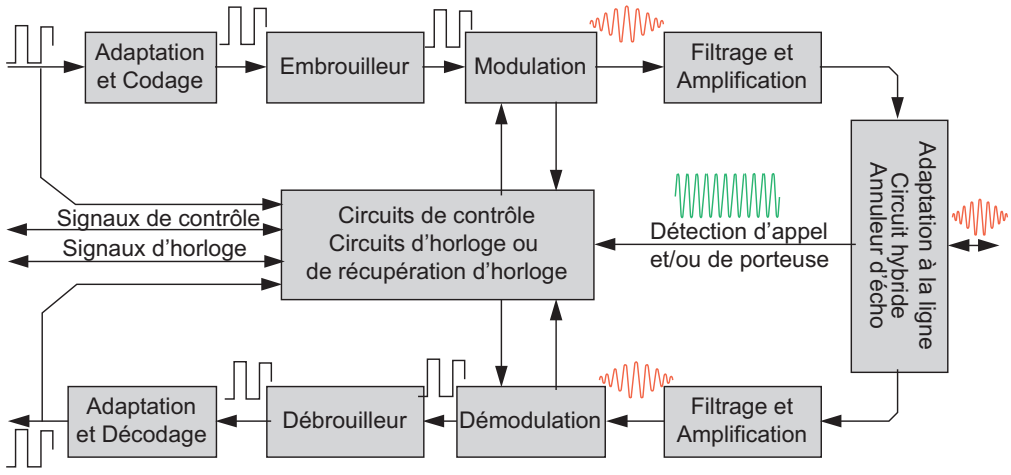


Figure 5.31 Synoptique simplifié d'un modem.

© Dunod – La photocopie non autorisée est un délit

En émission, un codeur fournit les valeurs multiniveaux au modulateur. En réception, la fonction inverse est réalisée. Le dialogue avec le terminal (ETTD) est contrôlé par un circuit spécialisé. Les principales caractéristiques d'un modem sont :

– le mode de travail, bande de base ou large bande (attention, rappelons que c'est par abus de langage qu'on appelle « modem bande de base » un ERBdB) ;
– le type de transmission, asynchrone ou synchrone, certains modems sont susceptibles de travailler dans les deux modes ;
– le débit binaire, les modems modernes testent la ligne et adaptent leur débit aux caractéristiques de celle-ci (bande passante, rapport signal à bruit) ;
– la rapidité de modulation qui permet de choisir, pour un débit donné, le modem le mieux adapté au support sur lequel il sera utilisé ;
– le support pour lequel il est prévu (RTC, liaison louée analogique à 2 ou 4 fils...) ;
– le mode de fonctionnement (*simplex*, *half duplex*, *full duplex*) ;
– le type de codage utilisé (ERBdB) ;
– le type de jonction (interface ETTD/ETCD).

Aucune normalisation n'a été édictée pour les ERBdB, ceux-ci doivent donc s'utiliser par paire de même référence et du même constructeur.

Le modem V.34

Le modem V.34 a introduit la notion d'adaptation du débit aux conditions de la ligne en cours de transmission. Le V.34 teste la qualité de la ligne en permanence et réalise l'adaptation des débits par pas de 2 400 bit/s. Le modem choisit en conséquence la meilleure porteuse parmi les 9 proposées par la norme. La figure 5.32 illustre les bandes de fréquences pouvant être utilisées (229-3 673 Hz), on remarquera que celles-ci peuvent excéder la bande traditionnelle de 300-3 400 Hz.

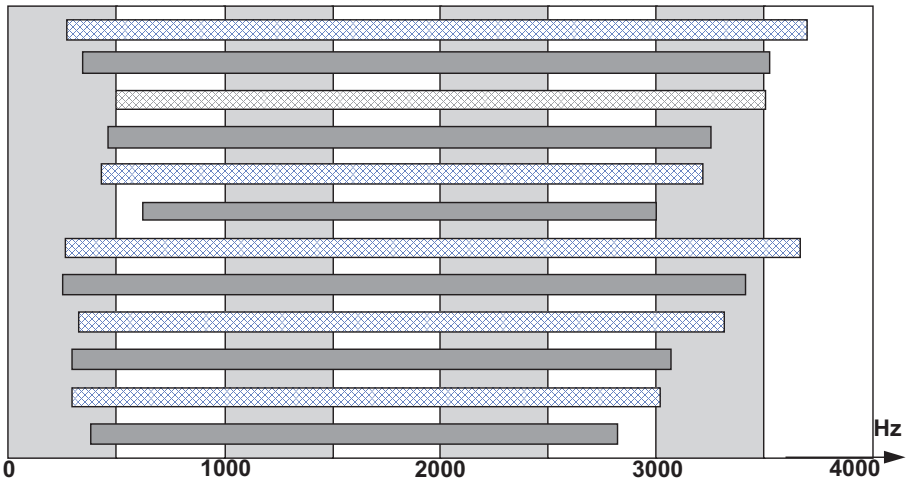


Figure 5.32 Bandes de fréquence définie par la norme V.34.

Le modem V.34 a introduit la transmission asymétrique avec basculement. En mode full duplex, le canal de transmission est divisé en deux sous-canaux, l'un lent et l'autre rapide. Le basculement des canaux est automatique, le modem offrant le plus de bande passante à la source lui soumettant le plus de données. Un canal spécifique est dédié aux données de service (test de lignes...). À l'origine définie pour un débit de 28 800 bit/s, la norme V.34 a évolué pour offrir des débits pouvant aller jusqu'à 33 600 bit/s (V.34+).

Le modem V.90

Le débit d'un modem est limité par le rapport signal à bruit de la liaison. La numérisation des réseaux a réduit considérablement le bruit de transmission. La liaison d'abonné en cuivre (boucle locale en téléphonie) et l'opération de numérisation du signal (bruit de quantification) sont les principales sources de bruit. Si l'une des extrémités est directement reliée en numérique au réseau, le bruit global de la liaison est réduit et le débit peut être supérieur. C'est le principe du modem V.90. C'est un modem dissymétrique. En effet, la liaison abonné vers **ISP** (*Internet Service Provider*) subit l'opération de quantification principale source de bruit, alors que le sens ISP vers abonné n'en subit pas. Le débit ISP vers abonné pourra, de ce fait, être supérieur au débit abonné/ISP (figure 5.33).

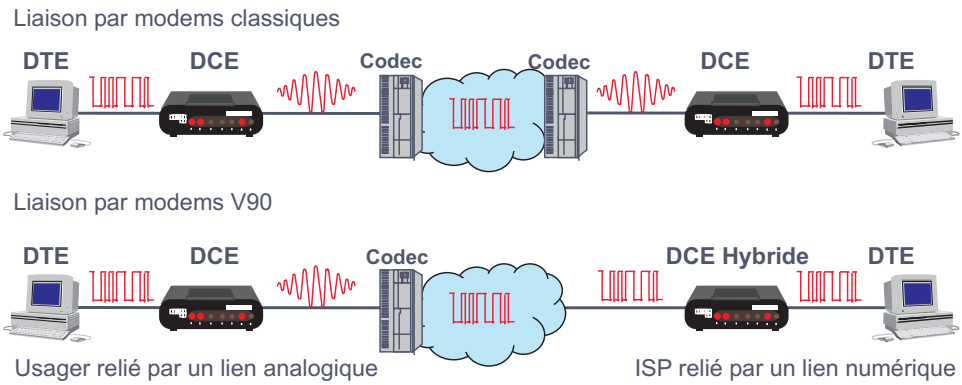


Figure 5.33 Modem classique et modem V.90.

L'avis V.90 autorise un débit brut de 56 kbit/s dans le sens ISP/usager et seulement de 33,6 kbits dans l'autre sens.

5.3.5 Principaux avis du CCITT

Le tableau de la figure 5.34 résume les principaux avis du CCITT (IUT-T).

Les modems les plus utilisés sont :

– V.34, V.32, V.32bis, V.22 et V.22 bis en transmission de données ;
– V.27ter, V.29 pour la télécopie (Fax) ;
– V.23 (Minitel) ;
– V.90, couramment utilisé pour les accès à Internet (modem dissymétrique 33/56 kbit/s).

© Dunod – La photocopie non autorisée est un délit

AVIS	Type Modulation	Débit	Mode de Transmission	Exploitation	Voie de retour	Support
V.21	Fréquence, 2 états	⩽ 300 bit/s	Asynchrone	Full Duplex		RTC, LS
V.22	Phase différentielle 4 états	2 400 bit/s 1 200 bit/s	Synchrone Asynchrone	Full Duplex		RTC LS
V.22 bis	MAQ 16 états	2 400 bit/s 1 200 bit/s	Synchrone Asynchrone	Full Duplex		RTC LS
V.23	Fréquence 2 états	⩽ 1 200 bit/s ⩽ 600 bit/s	Asynchrone Synchrone	Half Duplex et Full Duplex	optionnel 75 bauds	RTC LS
V.26	Phase différentielle 4 états	2 400 bit/s	Synchrone	Half Duplex et Full Duplex	optionnel 75 bauds	LS 4 fils
V.26 bis	Phase différentielle 4 états	2 400 bit/s 1 200 bit/s	Synchrone	Half Duplex Full Duplex	optionnel 75 bauds	RTC LS
V.26 ter	Phase différentielle 8 états	2 400 bit/s 1 200 bit/s	Synchrone Asynchrone	Full Duplex		RTC LS
V.27	Phase différentielle 8 états	4 800 bit/s	Synchrone	Full Duplex	optionnel 75 bauds	LS 4 fils
V.27 bis	Phase différentielle 8 états	4 800 bit/s 2 400 bit/s	Synchrone	Half Duplex Full Duplex	optionnel 75 bauds	RTC LS
V.27 ter	Phase différentielle 8 états	4 800 bit/s 2 400 bit/s	Synchrone	Half Duplex Full Duplex	optionnel 75 bauds	RTC LS
V.29	MAQ 16 états	9 600 bit/s 7 200 bit/s 4 800 bit/s	Synchrone	Full Duplex		LS 4 fils
V.32	MAQ 4 ou 32 états	9 600 bit/s 4 800 bit/s 2 400 bit/s	Synchrone Asynchrone	Full Duplex		RTC LS
V.32 bis		14 400 bit/s 12 000 bit/s 9 600 bit/s 7 200 bit/s 4 800 bit/s	Asynchrone Synchrone	Full Duplex		
V.33	MAQ	14 400 bit/s 12 000 bit/s	Synchrone	Full Duplex		LS 4 fils
V.34	MAQ 16, 32 ou 64 états	de 28 800 à 2 400 bit/s par bond de 2 400 bit/s	Synchrone Asynchrone	Half Duplex et Full Duplex		LS

Figure 5.34 Synthèse des principaux avis de IUT-T.

5.4 LA JONCTION DTE/DCE OU INTERFACE

5.4.1 Nécessité de définir une interface standard

La jonction ETTD-DTE/ETCD-DCE définit un ensemble de règles destinées à assurer la connectivité, le dialogue entre l'ETTD et l'ETCD (activation de la ligne...), la transmission des horloges, le transfert de données et le contrôle de celui-ci (figure 5.35).

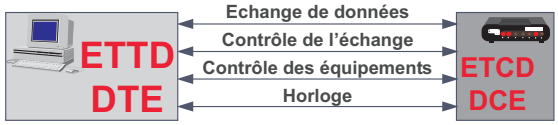


Figure 5.35 L'interface ou jonction ETTD/ETCD.

Une interface ETTD/ETCD spécifie :

– une interface mécanique qui fixe le connecteur physique ;
– une interface électrique qui détermine les niveaux électriques des signaux qui transitent par la jonction ;
– une interface fonctionnelle qui précise les fonctions remplies par telle ou telle broche : le transfert de données, les signaux de commande, les signaux de synchronisation et les masses ;
– enfin, une interface procédurale qui définit les procédures de commande et d'échange.

La normalisation des interfaces émane essentiellement de deux organismes : l'EIA (RS232, RS 449, RS 422, RS 423A...) et l'UIT (V.24, X.21, X.21bis...). Le tableau de la figure 5.36 présente les principales interfaces normalisées et leurs caractéristiques essentielles.

	Interfaces				
Appellation	**Mécanique**	**Électrique**	**Fonctionnelle**	**Portée**	**Débit nominal**
V.24/RS 232	ISO 2110 DB 25	V.28	V.24	12 m	2,4 à 19,2 kbit/s
V.35	ISO 2593 DB 34	V.11/V.10	V.24	15 m 10 m	48 à 64 kbit/s 128 à 256 kbit/s
V.36	ISO 4902 37 points	V.11/V.10	V.24	15 m 10 m	48 à 64 kbit/s 128 à 256 kbit/s
X.24/V.11	ISO 4903 DB15	V.11	X.24	100 m 50 m	64 à 1 024 kbit/s 1 920 kbit/s
G703	ETSI 300.166	G703	G703	300 m	2 048 kbit/s
G703/704	DB 9	G703	G704	300 m	256 à 1984 kbit/s

Figure 5.36 Les principales interfaces normalisées.

5.4.2 Les principales interfaces

Les interfaces mécaniques

De nombreux connecteurs ont été définis et associés à des interfaces spécifiques. La figure 5.37 représente les principaux connecteurs utilisés. D'origine Cannon, ils sont plus connus sous les appellations de DB25 pour le connecteur 25 broches, DB15 pour le connecteur 15 broches... que sous leurs appellations officielles attribuées par l'ISO (voir figure 5.36).

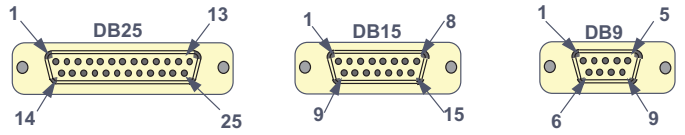


Figure 5.37 Les principaux connecteurs physiques.

La figure 5.37 présente les connecteurs de face, ils sont de type mâle (ceux qui ont des picots). Les micro-ordinateurs sont généralement équipés d'un connecteur DB25 femelle pour la liaison parallèle avec l'imprimante et d'un connecteur DB25 mâle pour la transmission de données. Ce dernier étant de plus en plus aujourd'hui remplacé par un connecteur DB9.

© Dunod – La photocopie non autorisée est un délit

Les interfaces électriques

Les interfaces électriques fixent les niveaux électriques des signaux et leur mode de transmission entre l'ETTD et l'ETCD. Les principaux avis sont :

– l'avis V.28 pour une interface en mode asymétrique (retour commun),

– l'avis V.10 (X.26) qui met en œuvre des niveaux de tension plus en adéquation avec l'intégration des circuits, utilise un mode asymétrique mais différentie la masse ETTD et ETCD.

– enfin, l'avis V.11 (X.27) qui reprend les niveaux électriques de l'avis V.10 mais en mode symétrique.

➤ L'avis V.28

En mode asymétrique, chaque fonction est matérialisée par un fil. L'information d'état est déduite de la différence de potentiel entre ce fil et la masse commune (terre de signalisation). Selon les différents niveaux, un courant résiduel peut circuler sur le fil de masse perturbant la transmission.

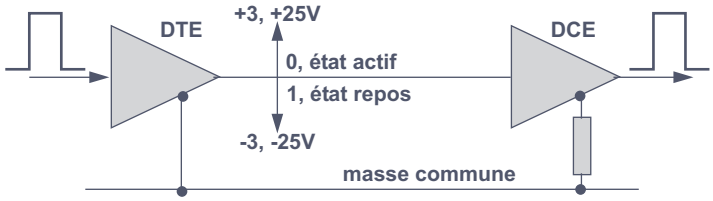


Figure 5.38 L'interface dissymétrique de l'avis V.28.

Les niveaux compris entre + 3V et – 3V ne doivent donner lieu à aucune interprétation, ce qui n'est pas toujours respecté.

L'avis V.10 est mieux adapté aux technologies modernes. Les tensions maximales sont de ± 5V. Les seuils de détection sont réduits à $V \leqslant -0{,}3V$ pour le 1 binaire et à $V \geqslant +0{,}3V$ pour le 0 binaire.

➤ L'avis V.11

L'avis V.11 devrait permettre d'atteindre des débits de l'ordre de la dizaine de Mbit/s sur une distance de quelques mètres (15 m).

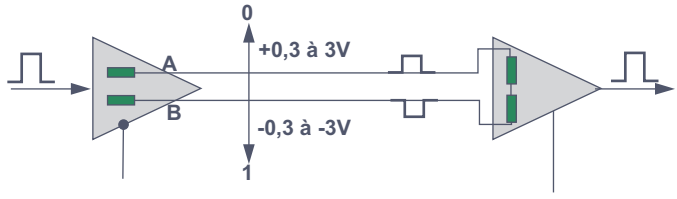


Figure 5.39 L'interface symétrique de l'avis V.11.

Chaque signal est défini par deux fils notés A et B, l'écart de tension maximal est de ± 5V. Les seuils de détection sont définis pour le 1 binaire $V_A - V_B \leqslant -0{,}3$ V et $V_A - V_B \geqslant +0{,}3V$ pour le 0 binaire.

Les interfaces fonctionnelles

Les interfaces fonctionnelles définissent un ensemble de circuits destinés à établir la liaison physique, la maintenir durant l'échange, assurer le transfert des données, fournir les signaux d'horloge et enfin rompre la liaison en fin d'échange.

➤ L'avis V.24

a) Description

L'avis V.24 (CCITT 1960, proche de la RS232C), utilise un connecteur Cannon DB25 (25 broches), il spécifie 4 types de signaux :

– des signaux de masse ;
– des signaux de transfert de données ;
– des signaux de commande ;
– des signaux de synchronisation.

Ceux-ci sont répartis en deux familles de circuits, chaque circuit ou signal est identifié par un numéro :

– les circuits de la série 100, la série 100 spécifie 39 circuits qui s'appliquent aux transmissions de données synchrones et asynchrones, aux services de transmission de données sur lignes louées à 2 ou à 4 fils en exploitation point à point ou multipoint ;
– les circuits de la série 200 pour les appels automatiques (devenu obsolète).

Les tableaux des figures 5.40, 5.41, 5.42, 5.43 fournissent la signification des principaux circuits et leur correspondance pour les interfaces V.24 du CCITT et RS232C de l'EIA.

		CCITT V.24		EIA RS-232 C		
Les circuits de masse						
Code	**Br**	**Abr.**	**Signification**	**Abr.**	**Signification**	**Fonction**
101	1	TP	Terre de protection	PG	*Protective groung*	
102	7	TS	Terre de signalisation	SG	*Signal ground*	Est utilisé comme retour commun en cas de jonction dissymétrique (V.24) ou comme potentiel de référence dans les jonctions symétriques (V.10, V.11, V.35).

Figure 5.40 Les signaux (circuits de masse) de la série 100.
Légende : **Code** N° attribué au circuit.
Br. N° de la broche utilisé sur un connecteur DB25.
Abr. Abréviation couramment utilisée pour désigner le circuit.

		CCITT V.24		EIA RS-232 C		
Les circuits de masse						
Code	**Br**	**Abr.**	**Signification**	**Abr.**	**Signification**	**Fonction**
103	2	ED	Émission de données	TD	*Transmitted data*	Circuit par lequel l'ETTD transmet à l'ETCD les données.
104	3	RD	Réception de données	RD	*Receive data*	Circuit par lequel l'ETCD transmet à l'ETTD les données reçues

Figure 5.41 Les signaux (circuits de transfert) de la série 100.

© Dunod – La photocopie non autorisée est un délit

		CCITT V.24		EIA RS-232 C		
Les circuits de commande						
Code	**Br**	**Abr.**	**Signification**	**Abr.**	**Signification**	**Fonction**
105	4	DPE	Demande pour émettre	RTS	*Request to send*	Circuit par lequel l'ETTD demande à l'ETCD de s'apprêter à recevoir des données, par le 103, pour les émettre sur la ligne.
106	5	PAE	Prêt à émettre	CTS	*Clear to send*	Circuit par lequel l'ETCD signale qu'il est prêt à émettre sur la ligne les données qui lui parviendront de l'ETTD.
107	6	PDP	Poste de données prêt	DSR	*Data set ready*	L'ETCD indique qu'il est en fonction et prêt à recevoir les commandes en provenance de l'ETTD.
108	20	TDP	Terminal de données prêt	DTR	*Data terminal ready*	108-1 Connecter le poste de données à la ligne, circuit par lequel l'ETTD demande à l'ETCD de se connecter à la ligne. 108-2 Équipement terminal de données prêt, circuit par lequel l'ETTD signale qu'il est en fonction, l'ETCD se met à son tour en fonction et se connecte à la ligne.
109	8	DS	Détection signal de ligne	CD	*Data carrier detect*	Signale que le signal reçu par l'ETCD est conforme à ce qu'il attendait
110	21	QS	Qualité du signal de données	SQD		Signale que des erreurs ont été reçues sur la voie de données.
111	23		Sélection débit ETTD		*DTE rate*	Est utilisé pour piloter l'ETCD lorsque celui-ci possède plusieurs débits.
112	18		Sélection débit ETCD		*DCE rate*	Indique à l'ETTD le débit binaire choisi quand l'ETCD possède plusieurs débits.
120	19		Demande à émettre		*Request to send*	Idem au 105, utilisé quand la voie de retour est utilisée.
125	22	IA	Indicateur d'appel	RI	*Ring Indicator*	Utilisé pour les appels automatiques, indique à l'ETTD que l'ETCD vient de détecter une demande de connexion.

Figure 5.42 Les signaux (circuits de commande) de la série 100.

Les signaux sont définis de manière identique du côté ETTD et ETCD, la liaison est dite **droite en point à point**. Ceci implique un comportement différent des équipements. En effet, le circuit 103, émission de données, vu de l'ETTD, correspond à une réception de données en provenance de l'ETCD. La figure 5.44 illustre une liaison complète, seuls les circuits les plus utilisés ont été représentés.

	CCITT V.24			EIA RS-232 C		
Les circuits de synchronisation						
Code	**Br**	**Abr.**	**Signification**	**Abr.**	**Signification**	**Fonction**
113	24		Horloge émission de l'ETTD		*DTE timing*	La base de temps pour le codage des signaux est fournie par l'ETTD
114	15		Horloge émission de l'ETCD		*DCE timing*	La base de temps est fournie par l'ETCD
115	17		Horloge réception de l'ETCD		*Receive timing*	La base de temps est fournie par l'ETCD
Les circuits de test						
140	21		Commande de test			Mise en œuvre de la boucle de test 2
141	18		Commande de test			Mise en œuvre de la boucle de test 3
142	25		Indication de test			Indique le bouclage et signale l'interdiction d'émettre des signaux.

Figure 5.43 Les signaux (circuits de synchronisation et de tests) de la série 100.

Les circuits d'horloge ont été volontairement omis. Les transmissions de données en mode asynchrone ne nécessitent aucune horloge. Les transmissions en mode synchrone exigent une référence d'horloge. L'horloge est transmise par un circuit spécifique. Elle peut être fournie par l'ETTD (DTE) ou l'ETCD (DCE). En réception, c'est toujours le DCE qui fournit l'horloge (circuit 115).

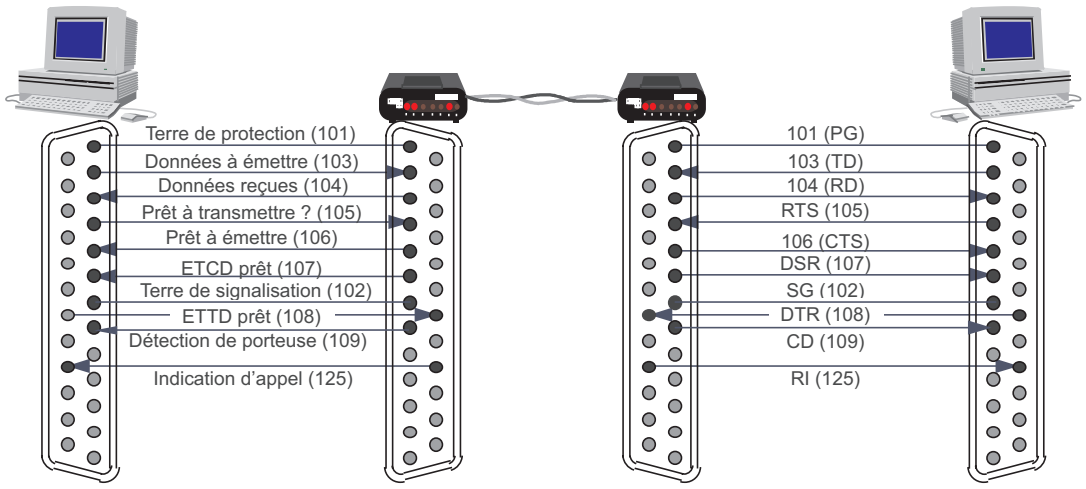


Figure 5.44 Les principaux circuits utilisés dans une liaison V.24.

En émission, l'horloge peut être fournie par le ETTD (circuit 113) ou l'ETCD, l'ETTD doit être paramétré en fonction du choix réalisé. En général, on préfère l'horloge de l'ETCD (DCE), le rythme de l'émission est ainsi adapté aux capacités du support (réseaux).

© Dunod – La photocopie non autorisée est un délit

b) Exemple de fonctionnement

L'interface ETTD/ETCD véhicule les signaux de contrôle et les données transmises. La procédure d'établissement de la liaison dépend du type de relation : liaison spécialisée, réseau téléphonique commuté avec ou non appel automatique et réponse automatique, liaison synchrone ou asynchrone... La figure 5.45 représente une connexion entre deux correspondants. La liaison est supposée *full duplex* et en mode asynchrone (pas de circuit d'horloge).

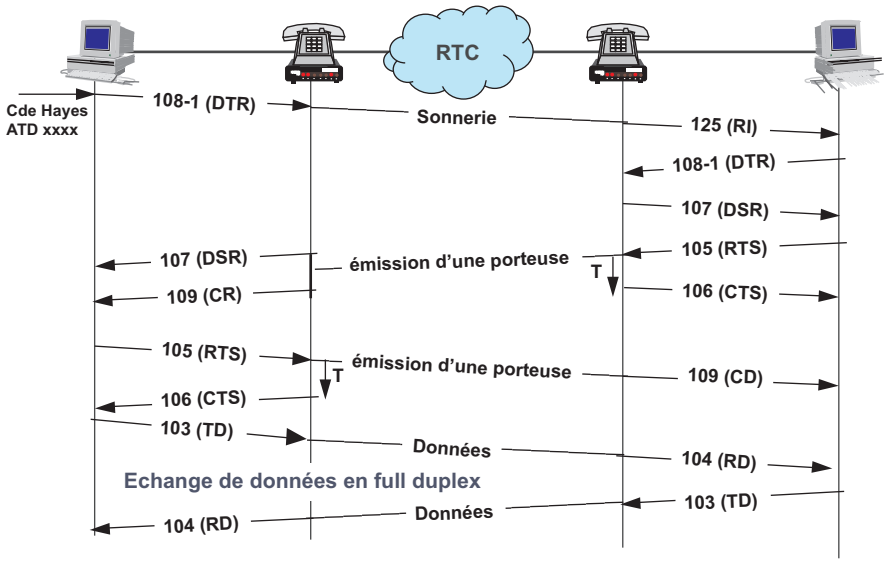


Figure 5.45 Exemple de dialogue ETTD/ETCD.

Les modems appelant et appelé sont sous tension et non connecté à la ligne. L'appelant reçoit une commande Hayes de demande d'appel. Non connecté à la ligne, il exécute la commande, prend la ligne (108-1), émet le numéro. Le modem distant, en attente de demande de connexion reçoit l'appel, il l'indique à son ETTD en levant le signal 125 (Indication d'appel ou **RI**, *Ring Indicator*). L'appelé accepte l'appel, demande à l'ETCD de se connecter à la ligne (108-1). La connexion réalisée l'ETCD signale qu'il est connecté à la ligne et prêt à recevoir des commandes (107).

L'ETTD appelé indique alors par le signal 105 (**RTS**, *Request To Send*) à son ETCD de se mettre en état de recevoir des données sur son circuit 103 (**TD**, *Transmitted Data*) afin de les émettre sur la ligne. L'ETCD se met en position d'émission, signale au distant qu'il va émettre des données par l'émission d'une porteuse (109, **CD** *Data Carrier Detect*). À réception de ce signal, l'appelé sait son appel accepté et signale à l'ETTD qu'il est connecté à la ligne et prêt à son tour à recevoir des commandes (107). Puis il indique à l'ETTD qu'il reçoit une porteuse du distant et que par conséquent celui-ci est prêt à transmettre. L'appelant procède comme l'appelé, demande de se mettre en position d'émission (105), l'ETCD envoie une porteuse et, après un délai (T), signale qu'en principe l'ETCD distant est prêt à recevoir et lui à émettre (106). L'échange de données peut alors avoir lieu.

Deux situations sont envisageables pour le modem appelé. Celle décrite ci-dessus correspond à l'utilisation dite 108-1. Le modem doit lever le signal 125 (Indication d'appel ou **RI**), pour que l'appelé décide ou non de monter le signal 108 (prendre la ligne ou **DTR**, *Data Terminal Ready*).

Une autre utilisation correspond à la levée anticipée du signal 108 (108-2), le modem est alors en attente d'appel. Lors de la réception d'un appel, celui-ci décroche automatiquement et signale la connexion par la levée du signal 107. Le signal 125 est alors inutile. En principe, une option de configuration du modem permet de choisir l'un ou l'autre fonctionnement.

Notons que, dans le cas d'une liaison *half duplex*, avant de « lever » le signal 105, l'ETTD vérifie que le signal 109 est « bas », c'est-à-dire, qu'il ne reçoit rien du distant. Supposons le 109 bas, en levant le signal 105, l'ETTD demande à son distant de se mettre en position de réception (109). La liaison est half duplex, c'est pour cette raison que la réponse de l'ETCD à la levée du signal 105 se fait sur temporisation. Le distant étant en position de réception ne peut acquitter cette demande. Ce temps (T) est appelé **temps de retournement** du modem. C'est le temps nécessaire pour passer d'une position d'émission en position de réception et inversement.

c) Éliminateur de modem

Lorsque l'on désire réaliser une connexion locale entre deux ordinateurs, il serait dommage de mobiliser deux modems pour réaliser la liaison. Un simple câble (figure 5.46) peut être utilisé pour mettre en relation les deux correspondants. Il suffit pour cela de croiser les fils émission et réception, d'où son appellation de câble croisé par opposition au câble droit utilisé pour connecter un ETTD à un ETCD (figure 5.46).

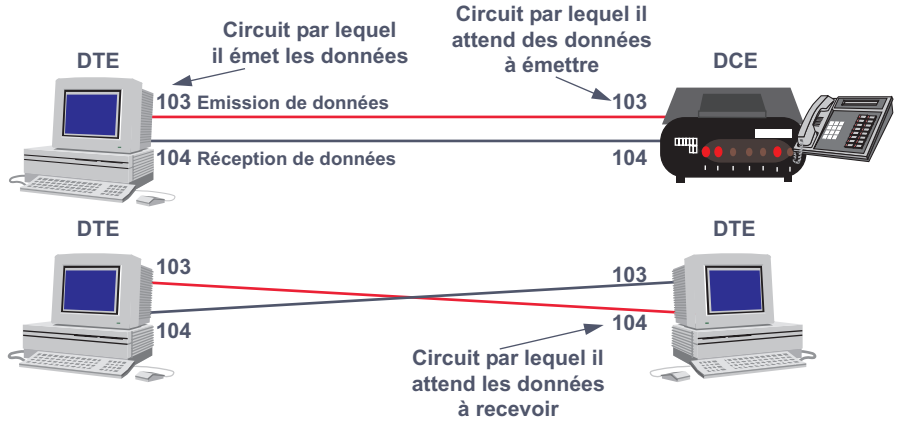


Figure 5.46 Notion de câble droit et de câble croisé.

Le schéma de la figure 5.46 représente ce que l'on nomme un éliminateur de modem. Trois fils suffisent (masse, émission et réception). Cependant, si les ETTD gèrent les signaux de commandes, il sera nécessaire de compléter le câblage par des bouclages locaux pour simuler le dialogue ETTD/ETCD, on réalise alors un câble appelé **null modem**.

Un équipement est dit avoir un comportement DTE quand il émet les données sur le 103 et les reçoit sur le 104, il est dit DCE dans une configuration inverse (émission sur le 104, réception sur le 103).

© Dunod – La photocopie non autorisée est un délit

L'interface d'accès aux réseaux publics

➤ L'interface X.21

Afin d'optimiser l'accès aux réseaux publics de données une nouvelle interface a été définie : l'avis X.21. Cette interface autorise des débits synchrones pouvant atteindre 10 Mbit/s sur quelques mètres et un temps d'établissement de la connexion d'environ 200 à 300 ms contre 3 à 15 s pour l'interface V.24.

L'avis X.21 définit l'interface d'accès entre un ETTD et un réseau public de transmission de données (figure 5.47), il fixe les règles d'échange pour :

– l'établissement de la connexion avec un ETTD distant à travers un ou plusieurs réseaux,

– l'échange des données en mode duplex synchrone,

– la libération de la connexion.

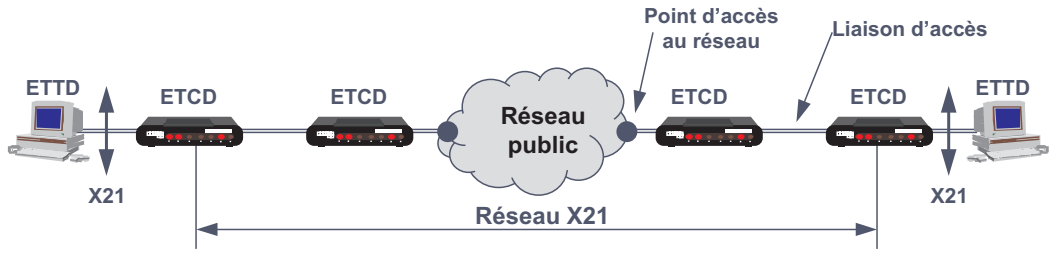


Figure 5.47 Le réseau X.21.

L'avis X.21 prévoit deux modes électriques de fonctionnement. Côté ETCD seul le mode équilibré peut être utilisé (2 fils par circuits), côté ETTD les deux modes sont possibles : le mode équilibré ou le mode non équilibré (retour commun). Il n'utilise que 8 circuits, les commandes ne sont pas matérialisées par des tensions sur un circuit spécifié mais par une combinaison de signaux. L'état de l'interface est indiqué par la combinaison des quatre circuits Transmission (T), Contrôle (C), Réception (R) et Indication (I). Le circuit C est activé par le terminal pour émettre l'appel et le circuit I par le réseau pour indiquer la connexion.

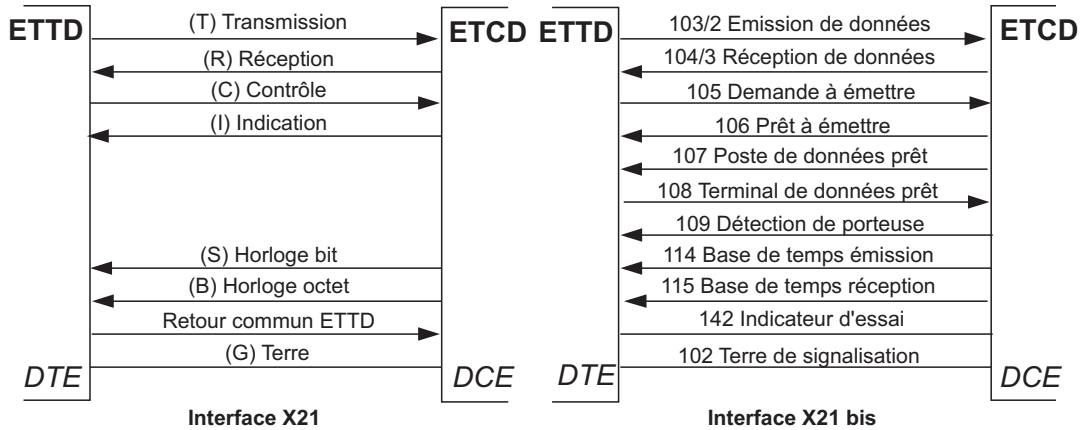


Figure 5.48 L'interface X.21 et X.21bis.

Malgré ses avantages, cette interface n'a pas connu un développement important. En effet, l'interface X.21 utilise un connecteur DB15 (ISO 4903) et la plupart des équipements sont équipés d'un connecteur DB25. Une adaptation a donc été réalisée : l'avis X.21 bis. Il consiste en une simplification de l'interface V.24. L'avis X.21 bis (figure 5.48) décrit l'accès à un réseau public au travers un connecteur DB25 (ISO 2110) ou DB34 (ISO 2593), il organise l'interfonctionnement de l'interface ETTD-ETCD.

X.21 est une interface de commandes logiques, alors que X.21 bis utilise les signaux fonctionnels de la V.24.

➤ L'accès au réseau téléphonique numérique

Les terminaux (téléphone, télécopieur...) des réseaux téléphoniques numériques (**RNIS**, Réseau Numérique à Intégration de Service ou **ISDN** *Integrated Services Digital Network*) sont raccordés à l'interface d'accès au réseau par un connecteur à contacts glissants : le connecteur RJ45 (figure 5.49). Le connecteur RJ45 (*Registered Jack*) est aussi utilisé dans les réseaux locaux.

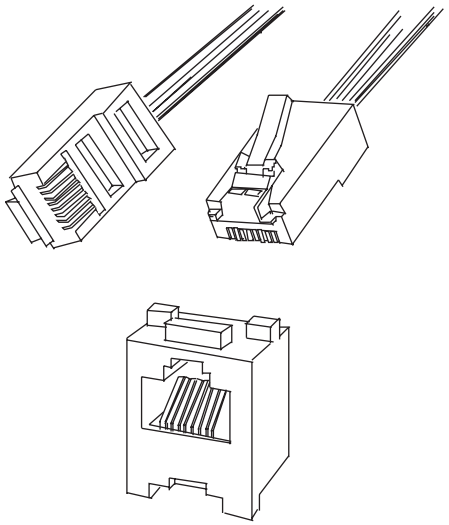


Figure 5.49 Le connecteur RJ45.

5.5 CONCLUSION

La limitation des débits est essentiellement due aux caractéristiques physiques des supports, mais les limites sont loin d'être atteintes. Les progrès des techniques de traitements du signal et de celles de codage des informations permettent d'améliorer la résistance au bruit et laissent espérer des débits se rapprochant de plus en plus des limites physiques. Cependant, les supports ne sont pas utilisés en permanence, la bande passante qu'ils offrent peut donc être partagée. L'étude des techniques de partage fait l'objet du chapitre suivant.

© Dunod – La photocopie non autorisée est un délit

EXERCICES

Exercice 5.1 Caractéristiques d'un modem

Un modem V.29 fonctionne à 9 600 bit/s sur un canal de bande passante (BP) de 500 à 2 900 Hz. On utilise une modulation de phase à 8 états avec une amplitude bivalente pour chaque état. Calculez :

a) la valence du signal modulé ;

b) la rapidité de modulation possible et celle utilisée ;

c) le rapport signal à bruit pour garantir le fonctionnement correct de ce modem.

Exercice 5.2 Débit possible sur un canal TV

Si un canal de télévision a une bande passante de 6 MHz, quel est le débit binaire possible en bit/s si on utilise un encodage de valence 4 ?

Exercice 5.3 Rapport Signal/Bruit

Appliquez la relation de Shannon à un circuit téléphonique et déterminez la capacité maximale théorique du canal, sachant que la bande passante est de 300-3 400 Hz et le rapport signal à bruit (S/B) est de 30 dB.

Exercice 5.4 Le null modem

Vous désirez relier deux ordinateurs par un câble. Le protocole d'échange de données gère les signaux de commandes : 105, 106, 107, 108, 109. Rappelez la fonction de chacun des circuits nécessaires et réalisez le schéma de câblage (le câble réalisé s'appelle un null modem).

Exercice 5.5 Contrôle de flux matériel

Par quels signaux l'ETTD ou ETCD peut signaler qu'il n'est plus en état de recevoir des données ?

Exercice 5.6 Modem dissymétrique

Les utilisateurs nomades d'une entreprise accèdent au réseau de celle-ci via le réseau téléphonique (RTPC, Réseau Téléphonique Public Commuté). L'établissement est relié au réseau téléphonique par une liaison numérique. Ce mode de liaison, lors de la transmission de données, permet l'économie d'une numérisation du signal, principale source de bruit (bruit de quantification). La liaison réalisée est dissymétrique, le bruit de quantification n'intervient que dans le sens Usager/Entreprise, ce procédé est mis en œuvre dans les modems V.90.

Dans toute liaison, chacun des composants participe au rapport signal sur bruit de l'ensemble. Pour cet exercice, on supposera que le rapport signal sur bruit de chacun des éléments constituant la liaison est indiqué par le tableau de la figure 5.50.

Élément	Rapport S/B
Boucle locale analogique (DCE-Codec)	2.10^5
Bruit de quantification du Codec (transformation analogique/numérique)	1.10^3
Réseau de transport (RTPC)	1.10^8
Boucle locale numérique (Réseau-DCE hybride ou MIC/PCM)	2.10^5

Figure 5.50 Rapport S/B de chaque élément participant à la liaison.

Le schéma ci-dessous (figure 5.51) représente la liaison utilisateur nomade/Entreprise.

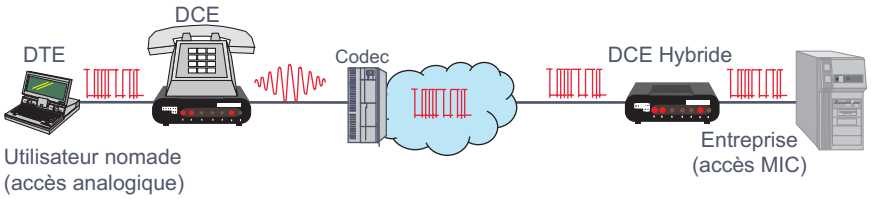


Figure 5.51 Liaison dissymétrique de type V.90.

Dans cette liaison le modem utilisateur nomade (modem analogique) génère un signal analogique et reçoit un signal modulé G.711. Le modem hybride, ou numérique, génère un signal G.711 et reçoit un signal analogique numérisé par le Codec source du bruit de quantification.

1) Sachant que le rapport signal sur bruit d'une liaison composée de n éléments est donné par la relation :

$$\left[\frac{S}{B}\right]^{-1} = \left[\frac{S1}{B1}\right]^{-1} + \left[\frac{S2}{B2}\right]^{-1} + \ldots + \left[\frac{Sn}{Bn}\right]^{-1}$$

Calculez :

a) le rapport S/B (signal/bruit) dans le sens Nomade/Entreprise ;

b) le rapport S/B dans le sens Entreprise/Nomade, on arrondira les valeurs à la puissance de 10 entière la plus faible.

2) Sachant, qu'un filtre passe-haut, en amont du Codec (Codeur/Décodeur) limite la bande passante de la liaison à 3 400 Hz, on vous demande :

a) de déterminer la rapidité de modulation envisageable sur cette liaison dans les deux sens ;

b) de calculer le débit maximal admissible dans chacun des deux sens ;

c) dans le sens Utilisateur/Entreprise le modem est classique et utilise une modulation de type MAQ, quel est le nombre d'états de celle-ci pour le débit normalisé maximal envisageable (on arrondira le $\log_2$ à la valeur entière la plus proche) ?

d) en admettant qu'il en soit de même dans le sens Entreprise/Utilisateur quel serait alors le nombre d'états ?

© Dunod – La photocopie non autorisée est un délit

Exercice 5.7 Rapidité de modulation

Quelle est la rapidité de modulation en bauds du signal sur un réseau local 802.3 10 base 5 (Ethernet, codage Manchester) lorsqu'il émet une suite continue de 1 ou de 0 ?

Chapitre **6**

Notions de protocoles

Dans les chapitres précédents nous avons étudié tous les mécanismes à mettre en œuvre pour transmettre un flot de bits entre deux systèmes distants. Cependant, il ne suffit pas de lire correctement les bits reçus, encore faut-il les traduire en données utilisables par les applications. On appelle protocole un ensemble de conventions préétablies pour réaliser un échange fiable de données entre deux entités (figure 6.1).

Figure 6.1 Un protocole organise l'échange de données.

Lors de l'échange de données, le protocole de transfert doit assurer :

- la délimitation des blocs de données échangés ;
- le contrôle de l'intégrité des données reçues[1] ;
- l'organisation et le contrôle de l'échange ;
- éventuellement le contrôle de la liaison.

1. Dans ce chapitre, le terme intégrité sera utilisé dans son sens le plus restrictif, il ne concernera que le contrôle d'erreur.

6.1 LA DÉLIMITATION DES DONNÉES

6.1.1 Notion de fanion

À l'instar des transmissions asynchrones où les bits de start et de stop encadrent les bits d'information, en transmission synchrone un caractère spécial ou une combinaison de bits particulière, le **fanion**, permet de repérer le début et la fin des données transmises (figure 6.2).

Figure 6.2 Délimitation des données par fanions.

Le fanion assure trois fonctions essentielles :

– il délimite les données ;
– émis en l'absence de données à émettre, il permet de maintenir la synchronisation de l'horloge réception ;
– dans le flot de bits transmis, le récepteur doit reconnaître les caractères. En identifiant le fanion, le récepteur peut se caler correctement sur une frontière d'octets (**synchronisation caractère**) et, par conséquent, traduire le flux de bits reçus en un flux d'octets.

6.1.2 Notion de transparence

L'utilisation d'un caractère spécifique pour indiquer le début ou la fin d'un bloc de données interdit l'usage de ce caractère dans le champ données. En conséquence, il faut prévoir un mécanisme particulier si on veut transmettre, en tant que données, le caractère ou la combinaison binaire représentative du fanion. Ce mécanisme se nomme **mécanisme de transparence** au caractère, si le fanion est un caractère, ou mécanisme de transparence binaire, si le fanion est une combinaison de bits.

Le mécanisme de transparence consiste à « baliser » le caractère à protéger par un autre caractère dit **caractère d'échappement**. Ce caractère inséré à l'émission devant le caractère à protéger (le faux fanion) doit lui-même être protégé s'il apparaît dans le champ données (figure 6.3).

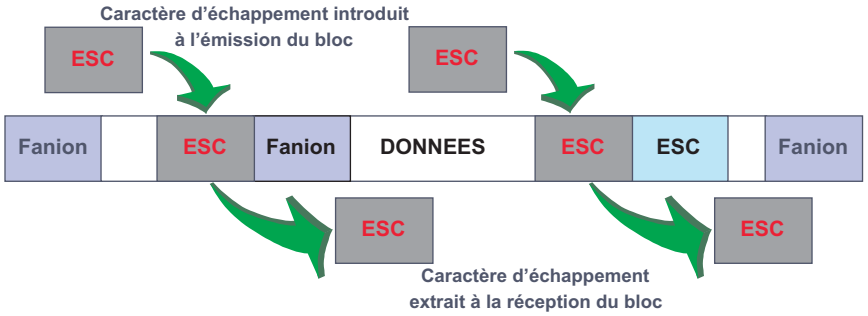


Figure 6.3 Principe de la transparence au caractère.

L'émetteur insère le caractère d'échappement devant le caractère à protéger. En réception, l'automate examine chaque caractère pour découvrir le fanion de fin. S'il rencontre le caractère d'échappement, il l'élimine et n'interprète pas le caractère qui le suit, il le délivre au système.

Certains protocoles utilisent les 32 premiers caractères du code ASCII pour assurer le contrôle de l'échange. Ces caractères sont dits caractères de commande, la transparence doit aussi être assurée pour ces caractères. Les protocoles qui utilisent des caractères pour le contrôle de l'échange sont dits **orientés caractères**. En principe, ils utilisent le caractère ASCII 16 (**DLE**, *Data Link Escape*) comme caractère d'échappement.

Dans d'autres protocoles, un champ particulier est réservé aux informations de contrôle. Ce champ peut contenir une combinaison binaire quelconque. Ces protocoles sont dits orientés bits. Dans ces protocoles le fanion est représenté par la combinaison binaire « 01111110 » soit 0x7E. La transparence binaire est assurée par l'insertion d'un « 0 » tous les 5 bits à « 1 » consécutifs. Seul, le fanion contiendra une combinaison binaire de plus de 5 bits à 1 consécutifs (01111110). Cette technique dite du **bit de bourrage** (*bit stuffing*), outre la transparence au fanion, permet la resynchronisation des horloges en interdisant les longues séquences de bits à 1 consécutifs. Les bits de bourrage insérés à l'émission sont éliminés par l'automate de réception. La figure 6.4 illustre le principe de la transparence binaire.

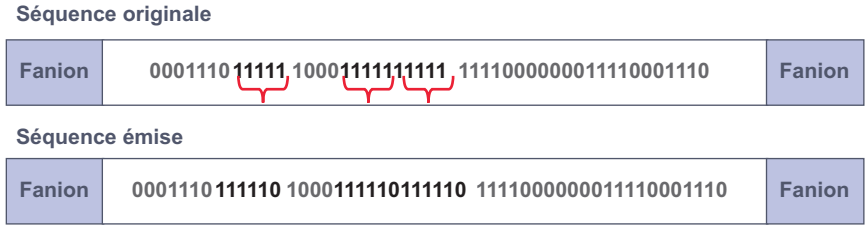


Figure 6.4 La technique du bit de bourrage.

Outre les délais introduits par l'insertion et l'élimination des bits ou caractères de transparence, cette technique modifie la taille des unités de données transmises. La longueur du bloc émis est variable, ce qui ralentit son traitement. Les protocoles dits à haut débit mettent en œuvre d'autres techniques, comme l'utilisation d'un codage de type 4B/5B, qui garantissent que le symbole choisi comme délimiteur ne pourra être présent dans le champ de données.

6.2 LE CONTRÔLE D'INTÉGRITÉ

D'une manière générale on doit, lors d'une transmission de données, s'assurer que les données reçues n'ont pas été altérées durant la transmission. Plusieurs facteurs peuvent modifier le contenu des données. Les uns sont d'origine humaine, le contrôle d'intégrité concerne alors la sécurité des données. Les autres sont d'origine physique, le contrôle d'intégrité porte alors le nom de contrôle d'erreur.

6.2.1 Notion d'erreur

Taux d'erreur binaire

Les rayonnements électromagnétiques, les perturbations propres au système (distorsions, bruit...) peuvent modifier les informations transmises (bits erronés). Compte tenu de l'exten-

© Dunod – La photocopie non autorisée est un délit

sion des réseaux et de l'utilisation massive de la fibre optique, la perte de la synchronisation des horloges est, aujourd'hui, la principale source d'erreurs.

On appelle **taux d'erreur binaire** ou **BER** (*Bit Error Rate*) le rapport entre le nombre d'informations (bits) erronées reçues et le nombre d'informations (bits) transmises.

$$Teb = \text{Nb d'info. (ou bits) erronées/Nb d'info. (ou bits) transmises}$$

Soit, par exemple, la transmission de la suite « 011001001100100101001010 » qui est reçue

« 011001101100101101000010 ».

Le message reçu diffère de 3 bits du message émis. Le nombre de bits émis est de 24 bits. Le taux d'erreur binaire (Teb) est de :

$$Teb = 3/24 = 0,125$$

Le taux d'erreur binaire varie en pratique de 10^{-4} (liaisons RTC[2]) à 10^{-9} (réseaux locaux). Dans les réseaux, les erreurs se produisent généralement par rafale. Le Teb exprime une grandeur statistique, l'erreur affecte aléatoirement n bits consécutifs et non 1 bit tous les x bits.

Si te est la probabilité pour qu'un bit soit erroné, la probabilité de recevoir un bit correct est de $(1 - te)$. Soit, pour un bloc de N bits, une probabilité de réception correcte (p) de :

$$p = (1 - te)(1 - te)...(1 - te) = (1 - te)^N$$

La probabilité de recevoir un bloc sans erreur est d'autant plus faible que la longueur du bloc est grande.

Par exemple, supposons une transaction de 100 caractères émis sur une liaison en mode synchrone à 4 800 bit/s avec un Teb de 10^{-4}. Les erreurs sont supposées être distribuées aléatoirement. Quelle est la probabilité de recevoir un message erroné ?

Le message de 100 caractères correspond à un bloc de :

$$100 \cdot 8 = 800 \text{ bits}$$

La probabilité de réception d'un bloc correct (Pc) est de :

$$Pc = (1 - 0,0001)^{800} = (0,9999)^{800} = 0,923$$

Soit la probabilité de recevoir un message erroné (Pe) :

$$Pe = 1 - 0,923 = 0,077$$

2. RTC, Réseau Téléphonique Commuté.

La détection d'erreur

On appelle détection d'erreur les mécanismes mis en œuvre pour que le système destinataire puisse vérifier la validité des données reçues. La détection d'erreur repose sur l'introduction d'une certaine redondance dans l'information transmise. Quatre techniques peuvent être mises en œuvre pour détecter et éventuellement corriger les erreurs :

– La **détection par écho**, le récepteur renvoie en écho le message reçu à l'émetteur. Si le message est différent de celui émis, l'émetteur retransmet le message. Cette technique est utilisée dans les terminaux asynchrones (Telnet, Minitel...).

– La **détection par répétition**, chaque message émis est suivi de sa réplique. Si les deux messages sont différents, le récepteur demande une retransmission. Cette technique est utilisée dans les milieux sécurisés très perturbés et dans certaines applications dites temps réel.

– La **détection d'erreur** par clé calculée, une information supplémentaire (clé) déduite des informations transmises est ajoutée à celles-ci (figure 6.5). En réception, le récepteur recalcule la clé, si le résultat obtenu correspond à la clé reçue les données sont réputées exactes, sinon le récepteur ignore les données reçues et éventuellement en demande la retransmission (reprise sur erreur).

– La **détection et correction d'erreur par code**, cette technique consiste à substituer aux caractères à transmettre, une combinaison binaire différente du codage de base (code autocorrecteur).

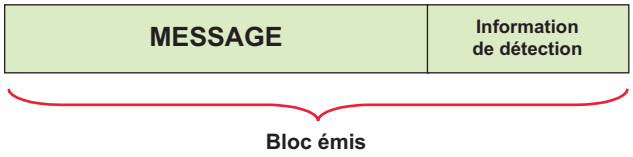


Figure 6.5 Principe de la correction d'erreur par redondance d'information.

6.2.2 Détection d'erreur par clé calculée

Principe

Dans les systèmes à clé calculée, une séquence de contrôle (CTL1) déduite d'une opération mathématique appliquée au message à émettre est envoyée avec le message. Le récepteur effectue la même opération. Si le résultat trouvé (CTL2) est identique à la clé calculée par la source (CTL1) le bloc est réputé exact, dans le cas contraire le bloc est rejeté (figure 6.6).

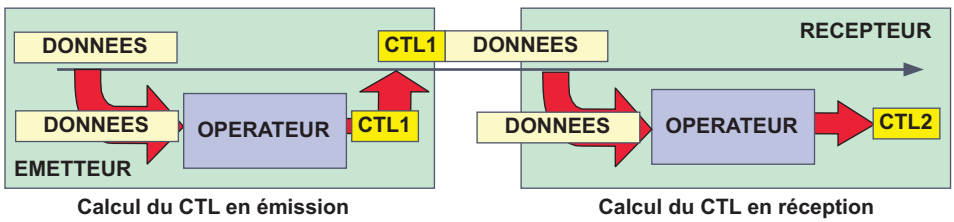


Figure 6.6 Principe de la détection d'erreur par clé calculée.

© Dunod – La photocopie non autorisée est un délit

Technique dite du bit de parité

La technique du **bit de parité** consiste à ajouter, à la séquence binaire à protéger, un bit, telle que la somme des bits à 1 transmis soit paire (bit de parité) ou impaire (bit d'imparité). Cette arithmétique modulo 2 est simple, mais elle n'introduit qu'une faible redondance. La protection apportée est limitée au caractère. La figure 6.7 illustre le mécanisme de calcul du bit de parité.

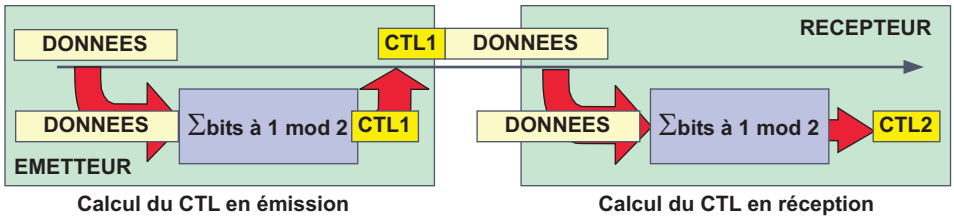


Figure 6.7 Mécanisme du bit de parité.

Le tableau de la figure 6.8 fournit quelques exemples de calcul du bit de parité. Les caractères ASCII (7 bits) sont protégés par l'introduction d'un 8e bit : le bit de parité.

Caractère	O	S	I
Bit 6	1	1	1
Bit 5	0	0	0
Bit 4	0	1	0
Bit 3	1	0	1
Bit 2	1	0	0
Bit 1	1	1	0
Bit 0	1	1	1
Bit de parité	1	0	1
Bit d'imparité	0	1	0

Figure 6.8 Exemple de calcul du bit de parité et d'imparité.

Cette technique, connue sous le nom de **VRC** (*Vertical Redundancy Check*), vérification par redondance verticale ne permet de détecter que les erreurs portant sur un nombre impair de bits. Elle est, essentiellement, utilisée dans les transmissions asynchrones (figure 6.9).

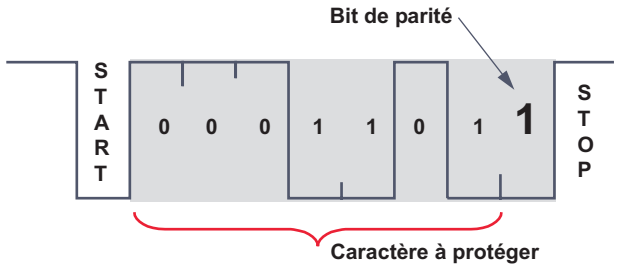


Figure 6.9 Le contrôle de parité dans les transmissions asynchrones.

Dans les transmissions synchrones, les caractères sont envoyés en blocs (figure 6.10). La technique du bit de parité est insuffisante, elle est complétée d'une autre information : le **LRC** (*Longitudinal Redundancy Check*).

Caractère à transmettre	**bit de parité**	Caractère à transmettre	**bit de parité**	...	Caractère LRC	**bit de parité**

Figure 6.10 Structure d'un bloc de caractères protégé par LRC.

Dans ce mode de contrôle dit de parité à deux dimensions, un caractère le LRC est ajouté au bloc transmis (figure 6.10). Chaque bit du caractère LRC correspond à la parité des bits de chaque caractère de même rang : le premier bit du LRC est la parité de tous les 1er bits de chaque caractère, le second de tous les 2e bits... Le caractère ainsi constitué est ajouté au message (figure 6.11). Le LRC est lui-même protégé par un bit de parité (VRC).

	H	**E**	**L**	**L**	**O**	***LRC* →**
bit 0	0	1	0	0	1	0
bit 1	0	0	0	0	1	1
bit 2	0	1	1	1	1	0
bit 3	1	0	1	1	1	0
bit 4	0	0	0	0	0	0
bit 5	0	0	0	0	0	0
bit 6	1	1	1	1	1	1
***VRC* ↓**	0	1	1	1	1	0

1001000	0	1000101	1	1001100	1	1001100	1	1001111	1	1000010	0
H		E		L		L		O		LRC	

Figure 6.11 Transmission du mot « HELLO ».

Dans l'ensemble (pile) de protocoles TCP/IP[3] utilisé par Internet, le mode de calcul du mot de contrôle se rapproche des techniques de parité. Le mot de contrôle sur 16 bits ou total de contrôle est le complément à 1 de la somme en complément à 1 des mots de 16 bits composant le message.

Les codes cycliques ou détection par clé calculée

Dans la détection par clé calculée, l'information redondante, la clé (**CRC**, *Cyclic Redundancy Check*), est déterminée par une opération mathématique complexe appliquée au bloc de données à transmettre et transmise avec celui-ci (figure 6.12).

Données : suite de bits quelconque.	Clé ou CRC ou FCS
Bloc ou TRAME à Transmettre	

Figure 6.12 Structure d'un bloc de bits protégé par clé calculée.

La méthode de contrôle par clé calculée considère le bloc de N bits à transmettre comme un polynôme de degré $N - 1 : P_{(x)}$. Ce polynôme est divisé par un autre, dit polynôme générateur $G_{(x)}$ selon les règles de l'arithmétique booléenne ou arithmétique modulo 2. Le reste de cette

3. TCP/IP (*Transmission Control Protocol/Internet Protocol*), cet ensemble de protocoles sera étudié en détail au chapitre 10.

© Dunod – La photocopie non autorisée est un délit

division $R_{(x)}$ constitue le CRC parfois appelé aussi **FCS** (*Frame Check Sequence*). Le CRC calculé est transmis à la suite du bloc de données (figure 6.12). En réception, le destinataire effectue la même opération sur le bloc reçu (figure 6.13). Le CRC transmis et celui calculé par le récepteur sont comparés, si les valeurs diffèrent une erreur est signalée.

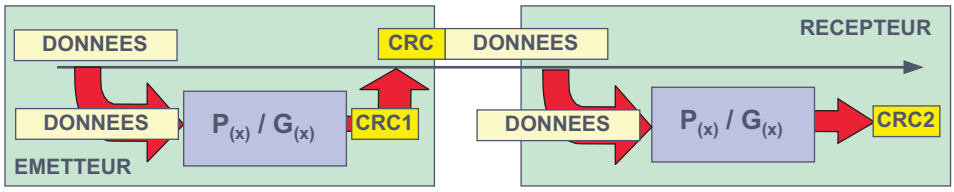


Figure 6.13 Principe de la détection d'erreur par clé calculée.

En réalité la méthode utilisée est quelque peu différente. En effet, si *D* est le dividende, *d* le diviseur et *R* le reste, la division $(D - R)/d$ donne un reste nul. En arithmétique booléenne, l'addition et la soustraction sont la même opération (figure 6.14), l'opération *(D – R)* est équivalente à l'opération *(D + R)*.

Addition

+	0	1
0	0	1
1	1	0

Soustraction

–	0	1
0	0	1
1	1	0

Multiplication

×	0	1
0	0	0
1	0	1

Figure 6.14 Les opérations booléennes.

Dans ces conditions (figure 6.15), la division par le polynôme générateur $(G_{(x)})$ de l'ensemble bloc de données et du CRC soit $P_{(x)} + R_{(x)}$ donne un reste égal à zéro. En réception, l'automate effectue la division sur l'ensemble du bloc de données y compris la clé calculée, lorsque le calcul du reste donne zéro et que le caractère suivant est le fanion, le bloc est réputé exact.

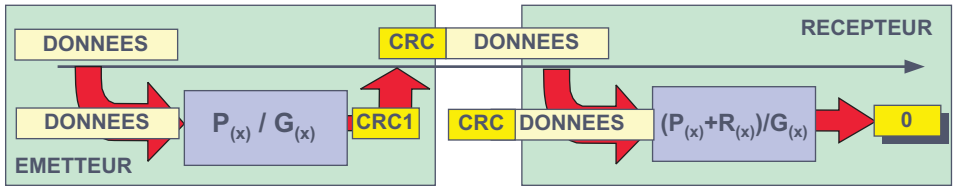


Figure 6.15 Détection d'erreur par CRC.

L'arithmétique modulo 2 est une arithmétique sans retenue, l'affirmation précédente n'est donc exacte que si le reste est ajouté à une séquence binaire nulle. Pour réaliser cette condition, avant d'effectuer la division, on multiplie le polynôme $P_{(x)}$ par x^m où m est le degré du polynôme générateur, ce qui correspond à une translation de m positions. Rappelons que le reste de la division par un diviseur de degré *m* est de degré *m – 1*, il comporte donc *m* termes. Cette opération a pour effet d'insérer *m* bits à zéro, pour y ajouter les termes du reste. L'exemple développé ci-dessous devrait éclairer le lecteur.

Exemple : on désire protéger le message « 110111 » par une clé calculée à l'aide du polynôme générateur $x^2 + x + 1$.

Au message 110111, on fait correspondre le polynôme :

$$x^5 + x^4 + 0x^3 + x^2 + x^1 + x^0$$

Pour permettre l'addition de la clé au message, on multiplie le polynôme représentatif du message par x^m où m est le degré du polynôme générateur. Le dividende devient :

$$(x^5 + x^4 + 0\,x^3 + x^2 + x^1 + 1).x^2 = x^7 + x^6 + 0x^5 + x^4 + x^3 + x^2 + \mathbf{0} + \mathbf{0}$$

$x^7 + x^6 + 0 + x^4 + x^3 + x^2 + \mathbf{0} + \mathbf{0}$	$x^2 + x + 1$
$x^7\ \ x^6\ \ x^5 \downarrow \downarrow \downarrow$	$x^5\ x^3\ 1$
$x^5\ \ x^4\ \ x^3 \downarrow$	
$x^5\ \ x^4\ \ x^3 \downarrow$	
$x^2\ \ 0\ \ 0$	
$x^2\ \ x\ \ 1$	
RESTE ⇒ $\mathbf{x\ \ 1}$	

Le reste de la division polynomiale est de degré inférieur à celui du diviseur, la division est terminée.

La division est réalisée par des systèmes « hardware » qui effectuent des « ou exclusif ». Aussi, appliquons la division par « ou exclusif » au polynôme 1010010111. Si le polynôme générateur est $x^4 + x^2 + x + 1$, il lui correspond la séquence binaire :

$$1(x^4) + 0(x^3) + 1(x^2) + 1(x^1) + 1(x^0) \quad \text{soit} \quad 10111$$

Multiplier par x^N, le polynôme représentatif du message, revient à ajouter N bits à 0 au message (voir exemple précédent). Le degré du polynôme générateur étant de 4, on ajoute 4 zéros à la trame de données (initialisation à zéro d'un registre à 4 positions). On obtient la division ci-dessous :

1 0 1 0 0 1 0 1 1 1 **0 0 0 0**	1 0 1 1 1
1 0 1 1 1	100 110 0100
0 0 0 1 1 1 0 1	Ce quotient est sans intérêt
1 0 1 1 1	
0 1 0 1 0 1	
1 0 1 1 1	
0 0 0 1 0 1 **0 0**	
1 0 1 **1 1**	
0 0 0 **1 1 0 0**	

Le reste (clé) comporte 4 termes, il est de degré – 1 par rapport au polynôme générateur. Le reste ou CRC4 est donc 1100. Le message à transmettre est $P_{(x)} + R_{(x)}$:

$$10100101111\mathbf{1100}$$

En réception, l'ensemble le message, données et clé, subit la même opération ; si le reste de la division est égal à zéro, on estime que le message n'a pas été affecté par une erreur de transmission. Vérifions cette affirmation sur l'exemple précédent :

© Dunod – La photocopie non autorisée est un délit

```
message              reste
1 0 1 0 0 1 0 1 1 1  1100  | 1 0 1 1 1
1 0 1 1 1                  |
0 0 0 1 1 1 0 1            |
      1 0 1 1 1            |
      0 1 0 1 1 1          |
        0 0 0 1 0 1  11    |
              1 0 1  11    |
              0 0 0  0000  |
```

Le message est réputé correctement transmis, le reste de la division (message + reste) est nul.

Exemples de polynômes générateurs

Déterminer un polynôme générateur consiste à rechercher une combinaison binaire telle que la probabilité de non-détection d'une erreur soit aussi faible que possible et que le calcul du CRC ne pénalise pas exagérément la transmission. Les polynômes générateurs utilisés font l'objet de normalisation. Le degré du polynôme est d'autant plus élevé que la probabilité d'apparition d'une erreur est grande c'est-à-dire que la longueur du bloc à protéger est importante. Les principaux polynômes employés sont :

– Protection de l'en-tête des cellules ATM[4],

$$x^8 + x^2 + x + 1$$

– Détection d'erreur couche AAL[5] type 3 et 4 d'ATM,

$$x^{10} + x^9 + x^5 + x^4 + x + 1$$

– Avis du CCITT N°41,

$$x^{16} + x^{12} + x^5 + 1$$

  – permet de détecter toutes les séquences d'erreurs de longueur égale ou inférieure à 16 bits,
  – permet de détecter toutes les séquences erronées comportant un nombre impair de bits,
  – permet de détecter 99,99 % des erreurs de longueur supérieure à 16 bits,
  – est utilisé dans HDLC[6].

– Comité IEEE 802[7],

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + 1$$

  – est utilisé dans les réseaux locaux.

4. ATM, *Asynchronous Transfert Mode*, protocole de transfert haut débit étudié au chapitre 10.
5. AAL, *ATM Adaptation Layer*, couche d'adaptation entre les protocoles de niveaux supérieurs et la couche ATM proprement dite.
6. HDLC, *High Data Link Control*, étudié dans la suite de ce chapitre
7. IEEE 802, comité de l'IEEE créé en 1980 (**80**) au mois de février (***2***) d'où 802 qui est spécialisé dans l'étude des réseaux locaux.

6.2.3 Les codes autocorrecteurs

Dans les systèmes autocorrecteurs, on substitue au mot à transmettre (mot naturel) un nouveau mot (mot code), tel que 2 mots codes successifs diffèrent de α bits, où α est appelé **distance de Hamming**. On montre que si la distance de Hamming est de α on peut :

– détecter toute erreur portant sur $(\alpha - 1)$ bits ;

– corriger toute erreur portant sur $(\alpha - 1)/2$ bits.

Dans la technique du bit de parité, la distance de Hamming est de 2. Cette technique ne permet pas la correction d'erreur, seule la détection d'erreur portant sur 1 bit est possible. En réalité, compte tenu de la spécificité du calcul du bit de parité, seules les erreurs portant sur un nombre impair de bits sont détectables.

Supposons le code de Hamming ci-dessous :

Mots naturels	Mots codes
00	10011
01	10100
10	01001
11	01110

Dans ce code, il y a toujours, au moins, 3 bits qui diffèrent d'un mot code à un autre, la distance de Hamming est de 3. Ce code permet donc de détecter toutes les erreurs portant sur 2 bits et de corriger toutes les erreurs ne portant que sur un seul bit.

Soit le mot 00 (figure 6.15), on transmet 10011, une erreur sur un bit correspond à la réception de l'un des mots suivants :

10010 10001 10111 11011 00011

Le mot reçu ne correspond à aucun des mots du code. Le code pouvant corriger toute erreur portant sur un bit, on considère que le mot transmis est celui du code dont la distance de Hamming n'est que de 1 avec le mot reçu. La figure 6.16 illustre ce propos, supposons que le mot reçu soit 11011. Seul le mot code 10011 est à une distance de Hamming de 1. La valeur reçue sera supposée être 10011, soit le mot origine 00.

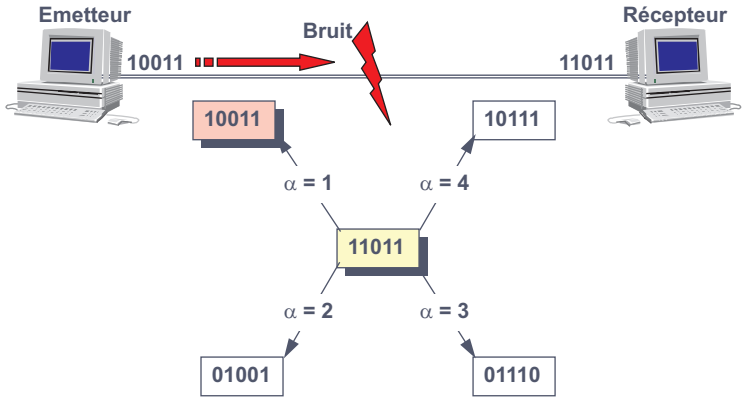


Figure 6.16 Estimation du mot reçu.

© Dunod – La photocopie non autorisée est un délit

6.3 LE CONTRÔLE DE L'ÉCHANGE

6.3.1 Du mode *Send and Wait* aux protocoles à anticipation

Les mécanismes de base

Le principe de base de toute transmission repose sur l'envoi (*Send*) d'un bloc d'information. L'émetteur s'arrête alors (*Stop*) dans l'attente (*Wait*) d'un accusé de réception. À la réception de l'acquittement, noté **ACK** pour *Acknowledge*, l'émetteur envoie le bloc suivant (figure 6.17 gauche).

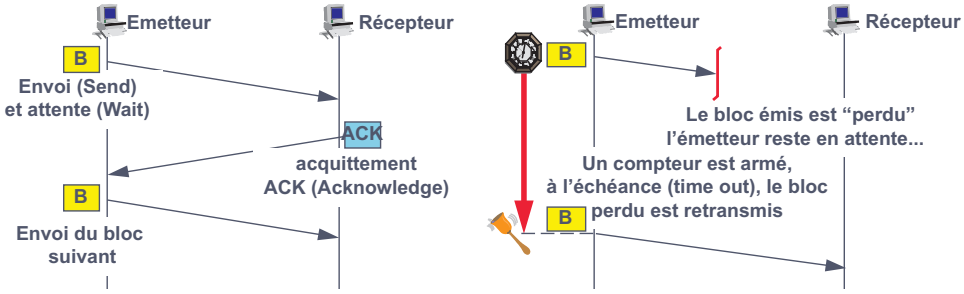


Figure 6.17 Le mode *Send et Wait* et la reprise sur temporisation.

En cas d'erreur de transmission, le bloc reçu est rejeté. Le bloc est dit perdu, il n'est pas acquitté. L'émetteur reste alors en attente. Pour éviter un blocage de la transmission, à l'émission de chaque bloc de données, l'émetteur arme un temporisateur (*Timer*). À l'échéance du temps imparti (*Time Out*), si aucun accusé de réception (ACK) n'a été reçu, l'émetteur retransmet le bloc non acquitté, cette technique porte le nom de reprise sur temporisation (**RTO**, *Retransmission Time Out*) ou correction d'erreur sur temporisation (figure 6.17 droite).

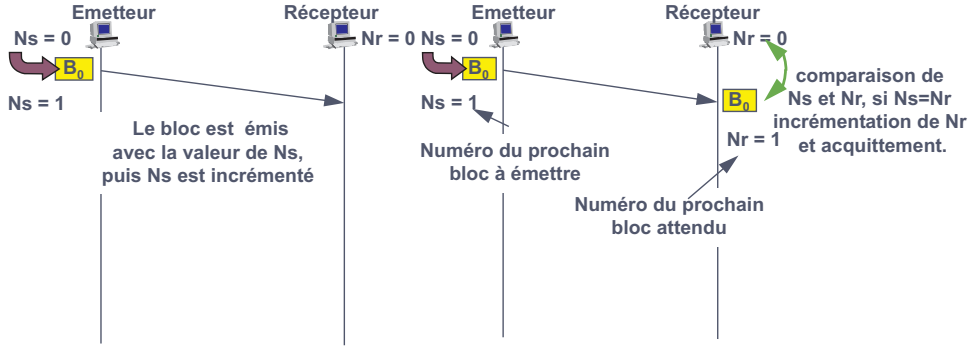


Figure 6.18 Numérotation des blocs de données.

Une difficulté survient si la perte concerne l'ACK. En effet, bien que les données aient été correctement reçues, l'émetteur les retransmet sur temporisation. Les informations sont ainsi reçues 2 fois. Pour éviter la duplication des données, il est nécessaire d'identifier les blocs. À cet effet, l'émetteur et le récepteur entretiennent des compteurs (figure 6.18). Les compteurs Ns (Ns, Numéro émis, s pour *send*) et Nr (Numéro du bloc à recevoir, r pour *receive*) sont

initialisés à zéro. Le contenu du compteur Ns est transmis avec le bloc, le récepteur compare ce numéro avec le contenu de son compteur Nr. Si les deux valeurs sont identiques le bloc est réputé valide et accepté. Si les valeurs diffèrent, le bloc reçu n'est pas celui attendu. Il est rejeté et acquitté s'il correspond à un bloc déjà reçu. Dans le cas contraire (Ns > Nr), il s'agit d'une erreur de transmission, nous verrons dans ce qui suit le comportement du récepteur dans ce cas (section 6.4.1). Cette numérotation évite la duplication et autorise le contrôle de séquencement des données reçues (figure 6.19).

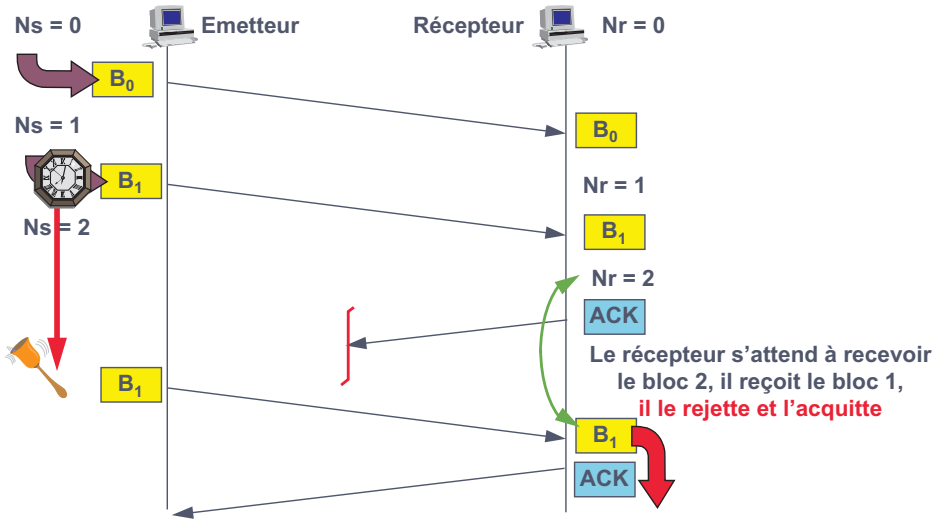


Figure 6.19 Contrôle de séquencement après une reprise sur temporisation.

Cependant, dans certains cas, le temps de traitement des données reçues est plus important que prévu ou (et) les délais de transmission sont devenus excessivement longs (figure 6.20).

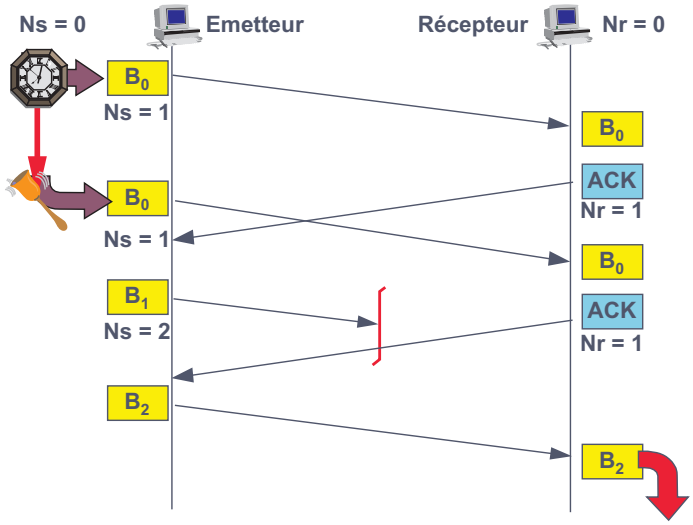


Figure 6.20 Délai d'acquittement trop important.

© Dunod – La photocopie non autorisée est un délit

Dans ces conditions, les données reçues peuvent ne pas être acquittées à temps. L'émetteur effectue alors une retransmission sur temporisation. Le récepteur ayant déjà reçu ces informations les élimine et les acquitte. En effet, pour le récepteur, s'il y a eu une retransmission, c'est que l'émetteur n'a pas reçu le précédent ACK. Ainsi, figure 6.20, à la réception du premier ACK (acquittant le bloc 0) l'émetteur envoie le bloc suivant (B1).

Supposons que ce bloc se perde, l'émetteur à la réception du second ACK (concernant le second envoi de B0) considère que cet ACK est relatif au bloc B1, il envoie le bloc suivant (B2). Ce bloc comporte un Ns différent du numéro attendu, il est rejeté. Pour éviter cette confusion d'interprétation, il est aussi nécessaire de numéroter les ACK.

Efficacité du protocole de base

Pour déterminer l'efficacité d'un protocole, il faut non seulement tenir compte des informations de contrôle (figure 6.21), mais aussi du délai d'acquittement. D'une manière générale, l'efficacité d'un protocole mesure le rapport du temps effectivement consacré à l'émission d'informations utiles au temps pendant lequel le support a été occupé, ou encore le rapport du nombre de bits utiles transmis au nombre de bits qui auraient pu être émis.

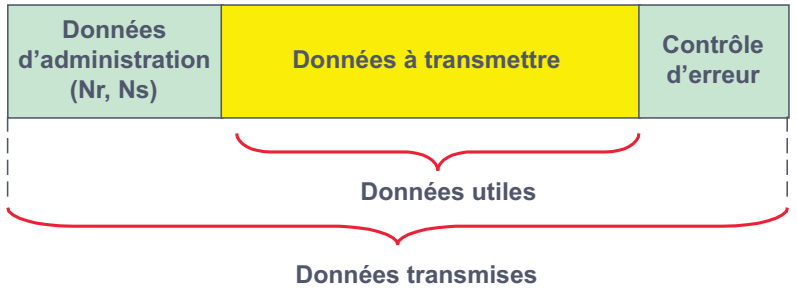


Figure 6.21 Structure de base d'un bloc d'information.

➤ La transmission étant considérée sans erreur

Considérons l'échange représenté par le diagramme temporel de la figure 6.22, on distingue les phases suivantes :

– l'émission du bloc de données, ou **U** représente les données utiles, **G** les données de gestion du protocole ;
– un temps mort pendant lequel l'émetteur attend l'acquittement qui correspond au temps de transit aller et retour sur le support et au temps de traitement des données reçues par le récepteur. Ce temps, généralement désigné sous le terme de temps de traversée des équipements, noté **RTT** (*Round Trip Time*, temps aller et retour), équivaut à l'émission de $(D \cdot RTT)$ bits où **D** représente le débit nominal du système ;
– enfin, la réception de l'accusé de réception de **K** bits.

Le temps entre l'émission du premier bit du bloc N et le premier bit du bloc suivant $(N + 1)$ est appelé temps d'attente et noté Ta.

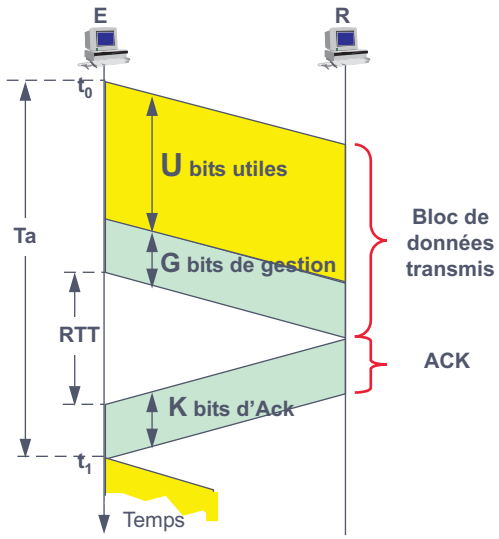


Figure 6.22 Efficacité du mode de base

Établissons l'efficacité du protocole dans une transmission sans erreur. Rappelons que l'efficacité d'un protocole (E) est le rapport entre le nombre de bits utiles transmis (U) au nombre de bits total transmis ou qui auraient pu être transmis (N).

$$E = U/N \qquad (1)$$

Le nombre de bits qui auraient pu être transmis entre t_0 et t_1 (Ta) s'exprime par la relation :

$$N = U + G + K + D \cdot RTT$$

Dès lors, on peut déterminer l'efficacité du protocole dans le cas où aucune erreur ne se produit, posons :

$$S = G + K + D \cdot RTT$$

$D \cdot RTT = Nb.$ de bits représentatifs du temps de traversée des équipements

G : bits de gestion (contrôle, adresse...)

K : bits d'accusé de réception

Soit, en reprenant l'équation (1) :

$$E_0 = U/N = U/(U + S)$$

E_0 : efficacité du protocole sans erreur

➤ Cas d'une transmission avec erreur

Si t_e (taux d'erreur) est la probabilité pour qu'un bit transmis soit erroné, $1 - t_e$ est la probabilité pour qu'un bit soit correctement transmis. Si la transmission porte sur N bits, la probabilité pour que N bits soient correctement transmis, est :

$$p = (1 - t_e)^N \quad \text{avec} \quad N = U + G.$$

© Dunod – La photocopie non autorisée est un délit

La probabilité pour que l'ACK soit correctement transmis est de :

$$p = (1 - t_e)^K$$

La probabilité pour qu'un bloc soit supposé correctement transmis est la probabilité composée :

$$p' = (1 - t_e)^N \cdot (1 - t_e)^K$$

L'efficacité du protocole avec erreur (E_{er}) est alors :

$$E_{er} = U \cdot (1 - t_e)^N \cdot (1 - t_e)^K / (U + S)$$

$$E_{er} = (U/U + S) \cdot (1 - t_e)^N \cdot (1 - t_e)^K$$

Soit :

$$E_{er} = E_0 \cdot (1 - t_e)^N \cdot (1 - t_e)^K = E_0(1 - t_e)^{N+K}$$

Or $K \ll N$, on peut donc admettre que l'efficacité en présence d'erreur est, par rapport à celle sans erreur :

$$E_{er} = E_0 \cdot (1 - t_e)^N$$

➤ Application numérique

Déterminons l'efficacité d'une transmission à 4 800 bit/s par blocs de 128 octets de données utiles, chaque bloc nécessite 6 octets de gestion ; l'accusé de réception comporte 6 octets. On considérera que le temps de traversée des équipements (RTT) est de 50 ms et que la liaison est affectée d'un taux d'erreur de 10^{-4}.

Calculons les bits représentatifs de la traversée des équipements :

$$N = D \cdot RTT = 4\,800 \cdot 50.10^{-3} = 240 \text{ bits}$$

Soit

$$S = G + K + D \cdot RTT = 8(6 + 6) + 240 = 336 \text{ bits}$$

L'efficacité sans erreur (E_0) est :

$$E_0 = U/(U + S) = 128 \cdot 8/(128 \cdot 8 + 336)$$

$$E_0 = 1\,024/(1\,024 + 336)$$

$$E_0 = 1\,024/1\,360$$

$$\boldsymbol{E_0 = 0{,}75}$$

Avec erreur (E_{er}) :

$$E_{er} = 0{,}75 \cdot (1 - t_e)^N \cdot (1 - t_e)^K$$

$$N = U + G$$

$$N = (128 + 6) \cdot 8$$

$$N = 1\,072$$

$$E_{er} = 0{,}75 \cdot (1 - 0{,}0001)^{1\,072} \cdot (0{,}9999)^{48}$$

$$E_{er} = 0{,}75 \cdot 0{,}89 \cdot 0{,}995$$

$$E_{er} = 0{,}667$$

$$\boldsymbol{E_{er} \approx 0{,}67}$$

Remarque : l'efficacité permet de déterminer le débit réel, c'est-à-dire le débit vu par l'application, celui-ci est donné par la relation :

$$\text{Débit réel} = \text{Débit nominal} \cdot \text{Efficacité réelle du protocole}$$

Les protocoles à anticipation

Les faibles performances du mode *Send and Wait* sont essentiellement dues au temps d'attente de l'ACK (T_t). Dans ces conditions, une amélioration substantielle peut être obtenue en émettant les blocs suivants sans attendre la réception des ACK, ce processus se nomme anticipation.

➤ Principe

Le principe est illustré par la figure 6.23. L'émetteur procède à l'émission continue des blocs. Cependant, pour autoriser une éventuelle retransmission après erreur (reprise sur erreur), il mémorise les blocs émis (mise en mémoire tampon ou *bufferisation*). À la réception de l'ACK d'un bloc émis, il libère le buffer[8] correspondant. La notion d'anticipation est limitée par le nombre de buffers que l'émetteur met à disposition du protocole.

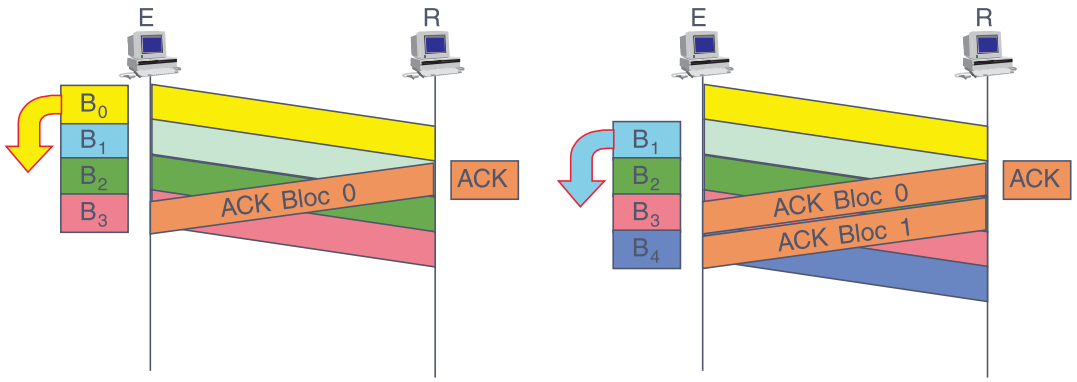


Figure 6.23 Principe des protocoles à anticipation.

On appelle fenêtre d'anticipation ou crédit d'émission, notée **W** (*Window*), le nombre de blocs que l'émetteur peut mémoriser en attente d'acquittement. L'efficacité de la transmission est maximale lorsqu'il n'y a pas d'arrêt de l'émission pendant le temps d'attente de l'ACK (émission continue). La taille de la fenêtre optimale correspond donc au nombre de blocs à transmettre pour que l'émission soit continue (figure 6.24).

8. Le terme buffer, en français mémoire tampon, est désormais passé dans le langage courant. Par la suite nous adopterons ce terme, car bufferisation est plus évocateur que tamponnage !

© Dunod – La photocopie non autorisée est un délit

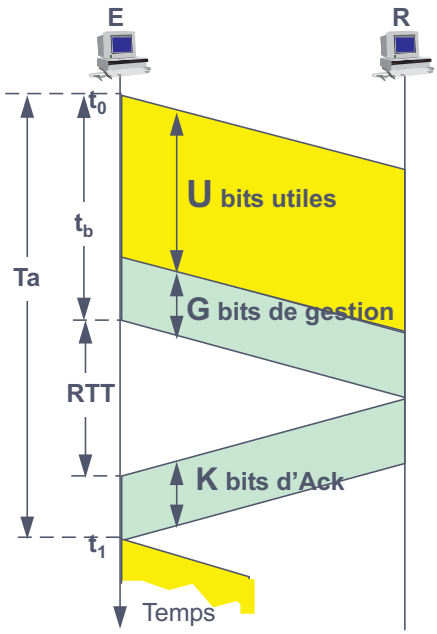


Figure 6.24 Détermination de la fenêtre.

Reprenons les paramètres définis au paragraphe précédent :

– Ta ou temps d'attente, temps entre l'émission du premier bit de la trame N et le premier bit de la trame $N + 1$ en mode *Send and Wait,*

– RTT temps de traversée des équipements,

et en nommant W la taille de la fenêtre, on obtient :

Si t_b représente le temps d'émission d'un bloc (volume à émettre sur débit) :

$$t_b = (U + G)/D$$

Il n'y aura pas d'arrêt des émissions si

$$W \cdot t_b \geqslant Ta$$

La taille optimale de la fenêtre est

$$W \geqslant Ta/t_b$$

➤ Modes de gestion de la fenêtre

Dans la figure 6.23, chaque bloc est acquitté. Lors de la réception d'un ACK, l'émetteur libère un buffer et émet le suivant. On dit que la fenêtre s'est ouverte de 1. Ainsi, dans la figure 6.25 nous supposons une fenêtre de 3, à réception de l'ACK0, le buffer B0 est libéré, l'émetteur transmet B4. À la réception de l'ACK1, B1 est libéré, l'émetteur émet B5... La fenêtre est dite **glissante**, dans l'hypothèse de la figure 6.25, la fenêtre est de 3, alors que la capacité de numérotation des blocs est de 8 (3 bits, numérotation modulo 8).

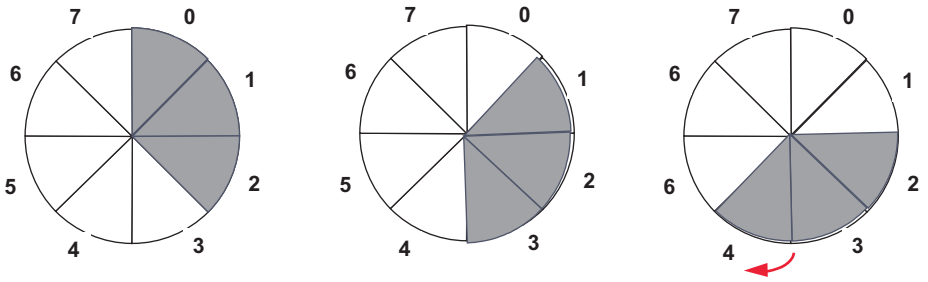


Figure 6.25 Gestion de la fenêtre dite « glissante ».

Cependant, chaque bloc n'a pas nécessairement besoin d'être acquitté individuellement. L'acquittement peut être différé et concerner plusieurs blocs. La figure 6.26 illustre ce propos. La fenêtre est de 3, l'acquittement du troisième bloc reçu (Nr = 3) acquitte les blocs 0, 1, 2 et demande l'émission du quatrième bloc qui portera le numéro 3. Nr représente le numéro du prochain bloc attendu. L'acquittement est dit global ou différé.

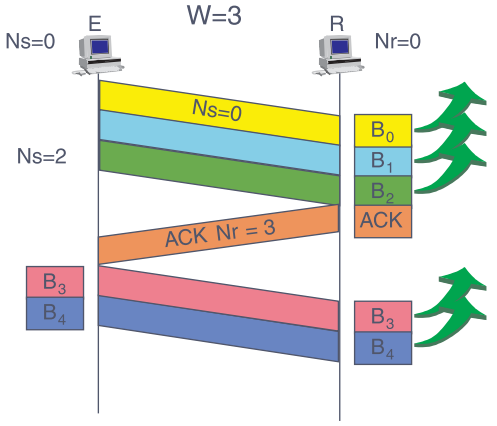


Figure 6.26 Principe de l'acquittement global ou différé.

Dans ce mode de fonctionnement, il y a arrêt des émissions quand le crédit d'émission est consommé. À la réception d'un ACK, la fenêtre se rouvre de tout le crédit, elle est dite **sautante** (figure 6.28).

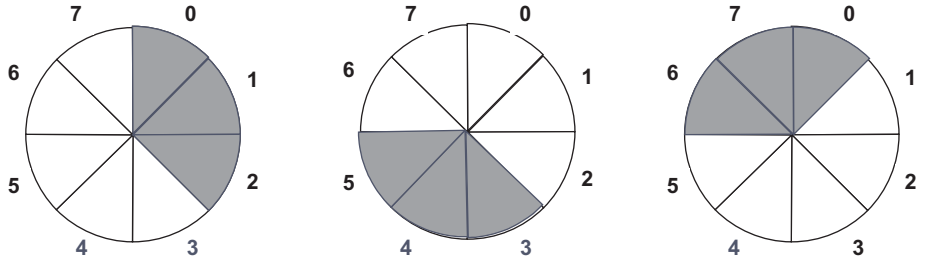


Figure 6.27 Gestion de la fenêtre dite « sautante ».

© Dunod – La photocopie non autorisée est un délit

➤ Les protocoles à fenêtre et la politique de reprise sur erreur

Le récepteur délivre les blocs reçus au fur et à mesure de leur réception. En cas d'erreur de transmission deux politiques de reprise sur erreur sont envisageables :

– le récepteur mémorise les blocs reçus hors séquencement, l'émetteur sur temporisation ou sur demande explicite du récepteur ne retransmet que le bloc erroné (figure 6.28 gauche) ;
– le récepteur rejette tous les blocs reçus hors séquencement, l'émetteur reprend alors la transmission à partir du bloc perdu, le protocole est dit **Go Back N**, ou N correspond au nombre de blocs retransmis (figure 6.28 droite).

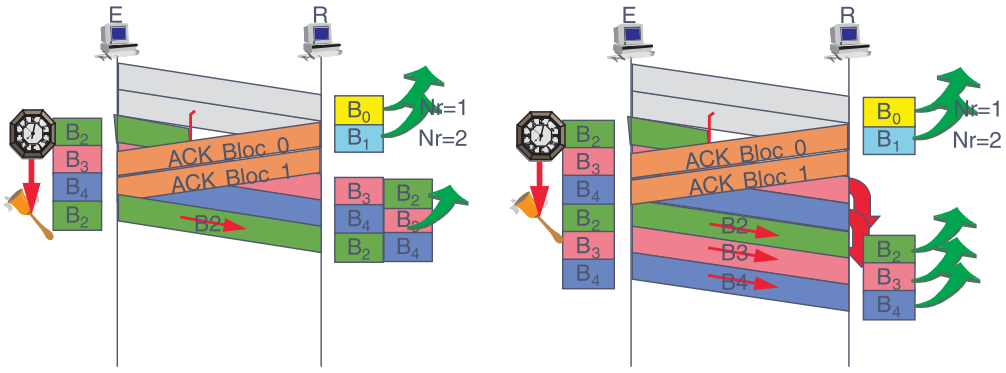


Figure 6.28 Les politiques de reprise sur erreur.

Dans la première hypothèse (figure de gauche), le rejet est qualifié de **rejet sélectif**, la transmission est optimisée mais nécessite des mémoires tampons importantes en réception (buffers) et le réordonnancement de tous les blocs. Le nombre de blocs déséquencés pouvant être reçus par le récepteur s'appelle **fenêtre de réception**.

Dans le second cas, la mémoire du récepteur est optimisée, la puissance de calcul du récepteur est minimisée, pas de reséquencement, mais la transmission est pénalisée par la retransmission de tous les blocs. Ce mode de reprise sur erreur est appelé **rejet simple**, la taille de la fenêtre de réception est alors de 1.

➤ Rejet simple ou rejet sélectif ?

À des fins de minimisation de mémoire, le rejet simple est généralement utilisé. Cependant, lorsque le temps de transit dans le système de transmission est important le rejet sélectif s'impose.

Supposons deux systèmes de transmission illustrés par la figure 6.29. L'un utilise un réseau terrestre, l'autre une liaison satellitaire. Calculons, dans les deux hypothèses, les conséquences d'une reprise sur erreur dans le cas de l'utilisation du rejet simple.

Pour cela, formulons les hypothèses suivantes :

– taille moyenne des unités de données 128 octets ;
– débit des liaisons 64 kbit/s ;
– le temps d'émission des ACK est négligeable ;
– l'erreur affecte le premier bloc de la fenêtre (hypothèse pessimiste).

Figure 6.29 Système de transmission et traitement des erreurs.

Pour déterminer l'influence de la reprise sur erreur, il nous faut connaître le nombre de blocs qui seront retransmis, ce qui correspond à la taille de la fenêtre ($W \geqslant T_a/T_b$) :

- Temps d'émission d'un bloc $T_b = (128 \cdot 8)/64\,000 = 16$ ms
- Temps d'attente (supposé, pour simplification, égal au RTT) :
  - Liaison terrestre 50 ms
  - Liaison satellitaire 500 ms
- Fenêtre :
  - Liaison terrestre W $\geqslant$ 50 /16 = 4
  - Liaison satellitaire W $\geqslant$ 500 /16 = 32

En cas d'erreur, le récepteur reçoit le bloc retransmis après un temps minimal de Ta (reprise sur temporisation), auquel il faut ajouter le temps de retransmission du ou des blocs à retransmettre et le temps de transit dans le réseau.

	Transmission terrestre	Transmission satellitaire
Ta	50 ms	500 ms
Retransmission	$4 \cdot 16 = 64$ ms	$32 \cdot 16 = 512$ ms
Temps de transit	25 ms	250 ms
Temps total	139 ms	1 262 ms

Figure 6.30 Temps de pénalisation de la transmission

Ce simple calcul montre l'inadéquation d'un système de reprise simple sur une liaison satellite. De plus, si l'on considère que le taux d'erreur sur des voies hertziennes est important, le rejet sélectif s'impose. En ce qui concerne les transmissions terrestres, le temps de reprise n'est pas négligeable ; cependant, pour minimiser l'espace mémoire dans les commutateurs des réseaux on lui préfère le rejet simple.

6.3.2 Le contrôle de flux

Définition

Le mécanisme de la fenêtre d'anticipation optimise la transmission mais ne prend pas en compte les capacités de réception du destinataire. L'émetteur ne doit envoyer des données que si le récepteur peut les recevoir. Lors d'une transmission, le destinataire met à disposition du transfert un certain nombre de mémoires tampons (buffers). Le récepteur peut, compte tenu d'autres tâches à réaliser, ne pas vider ses buffers suffisamment rapidement, des blocs peuvent ainsi être perdus (figure 6.31).

© Dunod – La photocopie non autorisée est un délit

Figure 6.31 Nécessité d'instaurer un contrôle de flux.

Le contrôle de flux consiste à asservir la cadence d'émission de l'émetteur sur les capacités de réception du récepteur. L'émetteur ne peut alors émettre plus de données que le récepteur ne peut en accepter.

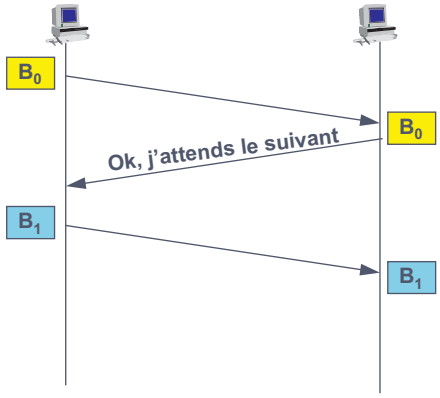


Figure 6.32 Principe du contrôle de flux

La figure 6.32 illustre le principe du contrôle de flux. Dans ce modèle, le récepteur délivre une autorisation explicite à l'émetteur avant l'émission de chaque bloc, le protocole est dit « XON, XOFF ». Le crédit ou fenêtre d'émission est dit de un.

Contrôle de flux par crédit d'émission

On appelle **crédit d'émission**[9], noté Ct, le nombre de blocs que l'émetteur est autorisé à transmettre. Deux politiques de gestion du contrôle de flux peuvent être envisagées (figure 6.33) :

– le contrôle de flux est dit **implicite** quand le crédit est prédéterminé (figure 6.33 gauche). Il reste constant durant toute la transmission (fenêtre statique). La transmission est optimisée par rapport au mode *Send and Wait*. Cependant, rien ne permet de garantir que le récepteur pourra toujours recevoir les N blocs du crédit. De plus, la transmission ne bénéficie pas d'éventuelles évolutions des capacités de réception du destinataire. Dans ce mode de fonctionnement, en cas de saturation, le récepteur envoie un message de demande d'arrêt des émissions.

9. La notion de crédit d'émission est souvent confondue avec celle de fenêtre d'anticipation. Bien que les concepts soient proches, la distinction doit être faite. La fenêtre d'émission est un paramètre fixé par l'émetteur alors que le crédit d'émission correspond à une autorisation d'émettre émanant du récepteur.

– le contrôle de flux est dit **explicite** ou **dynamique** lorsque le récepteur informe en permanence l'émetteur sur ses capacités de réception (figure 6.33 droite).

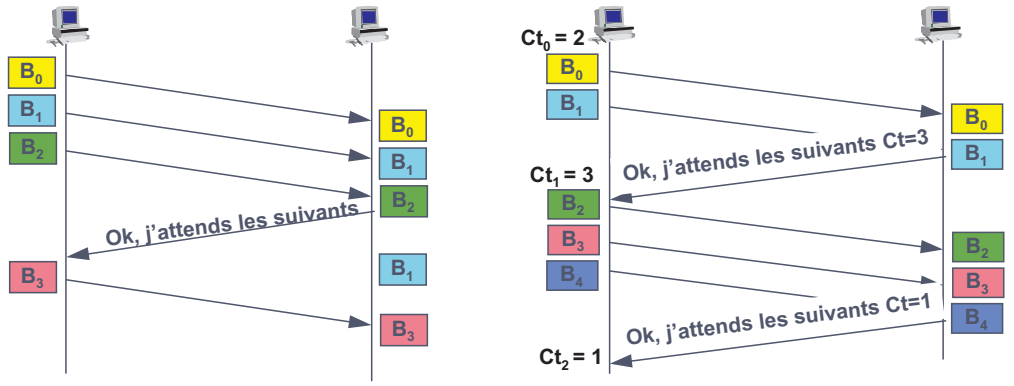


Figure 6.33 Contrôle de flux par fenêtre.

Les limites du contrôle de flux

La saturation du système peut intervenir avant que le crédit ne soit épuisé. De ce fait, les protocoles implémentent un mécanisme spécifique pour indiquer au système émetteur l'état de saturation du récepteur et arrêter les émissions de données. Cependant, entre le moment où le système reçoit un message saturant et le moment où l'émetteur en est averti, l'émission de données se poursuit. Aussi, pour examiner les limites du contrôle de flux, il convient de déterminer l'inertie du système, c'est-à-dire le nombre de messages envoyés et perdus. Ce nombre correspond à la fenêtre telle que nous l'avons définie précédemment. Aussi, déterminons la fenêtre d'émission d'un réseau haut débit en formulant les hypothèses suivantes (figure 6.34) :

– la distance internoeud est de 100 km ;
– le débit des liens est de 155 Mbit/s ;
– la longueur moyenne des blocs de données est de 100 octets ;
– les temps d'acquisition des données reçues et d'émission de l'ACK seront considérés comme négligeable.

Après saturation des buffers du récepteur, le délai qui sépare la réception de la demande de ralentissement ou d'arrêt des émissions est de Ta. Pendant ce temps, l'émetteur a poursuivi ses émissions, et a émis un nombre de blocs correspondant à la fenêtre. Calculons cette fenêtre :

Temps d'émission d'un bloc :

$$t_b = \text{Volume}/\text{Débit} = (100 \times 8)/155 \cdot 10^6 = 5 \cdot 10^{-6}\ \text{s}$$

Temps d'attente (si on admet une vitesse de propagation de $2 \cdot 10^8$ m/s) :

$$T_a = \text{Distance aller et retour}/\text{Vitesse} = 2 \cdot 10^5/2 \cdot 10^8 = 10^{-3}\ \text{s}$$

Fenêtre :

$$W = T_a/t_b = 10^{-3}/5 \cdot 10^{-6} = 200 \text{ blocs}$$

© Dunod – La photocopie non autorisée est un délit

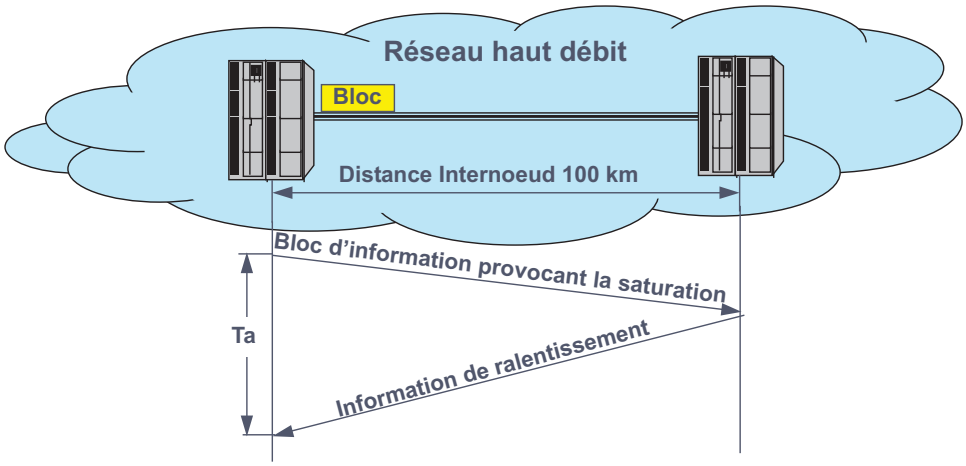


Figure 6.34 Contrôle de flux et débit élevé.

Lors de la perte d'un bloc par saturation des buffers, l'émetteur continue d'envoyer 200 blocs avant de recevoir l'information de demande de ralentissement. Devant une telle fenêtre, le temps de réaction est trop important. De plus, le ralentissement de la source est incompatible avec le transport d'informations dites temps réel comme la voix (réseaux voix/données).

Le contrôle de flux par fenêtre n'est efficace que pour des débits relativement faibles, ce qui l'élimine dans la plupart des réseaux modernes où aucun contrôle de flux n'est réalisé dans les réseaux. Cependant, les débits d'accès aux réseaux sont généralement faibles devant les débits internes au réseau, il est donc envisageable d'instaurer un contrôle de flux à l'interface usager. Une autre solution consiste à confier aux systèmes d'extrémité cette tâche (figure 6.35).

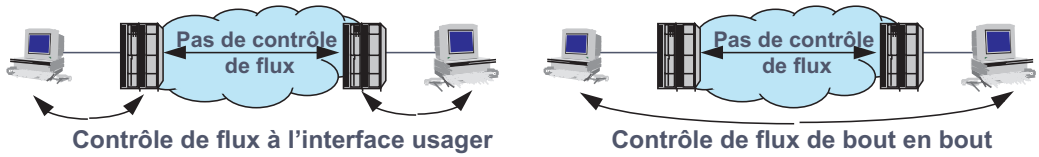


Figure 6.35 Contrôle de flux et débit élevé.

6.4 LA SIGNALISATION

6.4.1 Définition

Pour réaliser un transfert de données, il est nécessaire d'établir une liaison, de la contrôler durant l'échange et de libérer les ressources monopolisées en fin de communication. L'ensemble de ces informations de supervision de la liaison constitue la **signalisation**.

On distingue deux procédés pour l'acheminement des informations de signalisation :

– la signalisation dans la bande ;

– la signalisation par canal dédié ou hors bande.

6.4.2 La signalisation dans la bande

Dans la signalisation dite dans la bande, les informations de signalisation empruntent le même canal de communication que les unités de données. Ces informations sont transportées dans une structure de bloc identique à celle utilisée pour le transfert de données. Un champ spécifique, dénommé type d'unité de données, doit alors identifier la nature des informations transportées : informations de signalisation ou données. La figure 6.36 illustre ce principe.

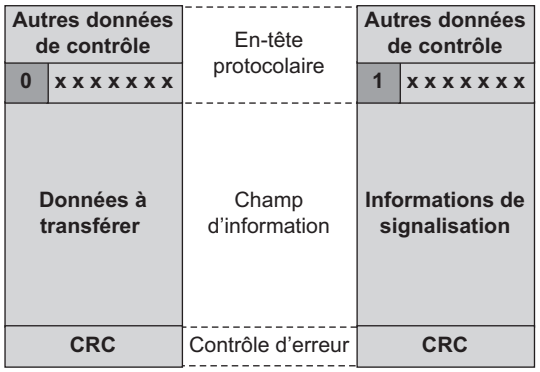


Figure 6.36 Unité de données et unité de signalisation.

Dans cet exemple (figure 6.36) le premier bit du champ type d'unité de données permet de distinguer une unité de données à transférer (bit à 0), d'une unité de transport d'informations de signalisation (bit à 1). Les autres bits de ce champ peuvent être utilisés pour distinguer différents types d'informations de signalisation. Le champ données est alors généralement vide, il peut cependant contenir des informations complémentaires comme la cause de rupture de la liaison logique...

Une autre possibilité, utilisée par le système de téléphonie d'Amérique du Nord, consiste à substituer à des bits de données, des bits de signalisation (signalisation par vol de bits). Ainsi, par exemple, le système de téléphonie d'Amérique du Nord et du Japon substitue, toutes les 6 IT, au bit de poids faible de parole un bit de signalisation. Ce système n'altère pas de façon audible la qualité de transmission, et offre un débit d'un peu plus de 1 kbit/s aux informations de signalisation.

La signalisation dans la bande est un procédé simple, mais la distinction des deux types d'unité de données pénalise le processus de commutation (interprétation des en-têtes). De ce fait, les informations transportées seront réduites à ce qui est strictement nécessaire, la signalisation est dite pauvre.

6.4.3 La signalisation hors bande

La signalisation par canal dédié distingue, lors d'une communication, deux voies : une voie pour le transfert de données (canal de données) et une voie pour les informations de signalisation (canal de signalisation). Ces deux voies pouvant être physiquement distinctes ou utiliser

© Dunod – La photocopie non autorisée est un délit

le même support physique, on parle alors de **voies virtuelles**[10]. Dans un tel système, illustré figure 6.37, le canal de signalisation est établi en permanence, alors que le canal de données peut n'être établi qu'à la demande.

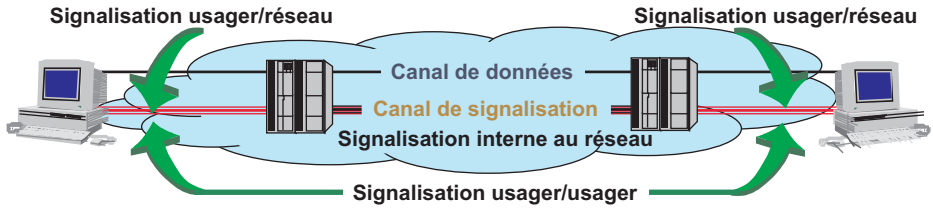


Figure 6.37 Signalisation par canal dédié à la signalisation.

La signalisation par canal dédié utilise un protocole différent du protocole de transfert de données : le protocole de signalisation. L'indépendance de ce protocole permet de multiplier les informations transmises. Ainsi, il devient possible de distinguer différentes signalisations :

– la **signalisation usager/réseau**, chargée essentiellement de l'établissement de la liaison usager/réseau et de sa supervision ;
– la **signalisation interne au réseau** qui permet l'établissement d'une liaison à travers le réseau (routage ou acheminement) et de la contrôler durant l'échange ;
– la **signalisation usager/usager** dite aussi de **bout en bout**. Cette signalisation permet aux entités distantes de s'échanger des informations hors du protocole de transmission. C'est ainsi qu'il est possible de transmettre, via le protocole usager/usager de petites quantités d'information en l'absence de toute communication établie.

Le Réseau téléphonique Numérique à Intégration de Service (**RNIS**) met aussi en œuvre ce type de signalisation. Cette approche est aussi utilisée dans tous les protocoles haut débit comme le **Frame Relay**[11] ou l'**ATM** (protocoles issus des travaux sur le RNIS Large Bande).

Figure 6.38 La signalisation par canal dédié.

Lorsque le support de communication est capable d'acheminer plusieurs communications, la signalisation des différentes communications peut être acheminée par un canal associé à chaque voie de communication. On parle alors de signalisation voie par voie ou **CAS**, *Channel Associated Signalling* (figure 6.38 gauche). Elle peut aussi être acheminée dans un canal

10. Nous montrerons au chapitre 7, lors de l'étude du multiplexage, comment sur une même voie physique on peut réaliser plusieurs canaux de communication (voies logiques).
11. Voir chapitre 11, section 11.2.4 et 11.2.5.

commun à toutes les voies de communication, on parle alors de signalisation par **canal sémaphore** ou **CCS**, *Common Channel Signalling*.

Le réseau téléphonique commuté utilise une signalisation de type CAS, alors que le réseau téléphonique à intégration de service met en œuvre une signalisation de type CCS.

6.5 ÉTUDE SUCCINCTE D'UN PROTOCOLE DE TRANSMISSION (HDLC)

6.5.1 Généralités

HDLC (*High Level Data Link Control*) est un protocole ligne dit de **point à point**. Dérivé de SDLC (*Synchronous Data Link Control*) d'IBM, il a été normalisé par le CCITT (UIT-T) en 1976.

L'unité de transfert d'HDLC est la trame (*Frame*), chaque trame est délimitée par un caractère spécifique : le fanion ou *Flag*. Ce caractère est le seul caractère spécial utilisé par le protocole. Le fanion est aussi employé pour maintenir, en l'absence de données à transmettre, la synchronisation entre les trames. La figure 6.39 représente le principe d'une liaison HDLC. Les symboles « F » représentent les fanions envoyés durant les silences pour maintenir la synchronisation. L'entité primaire désigne celui qui a initialisé la communication. Quand chaque entité peut initialiser la communication et émettre des commandes, le mode de fonctionnement est dit **équilibré**.

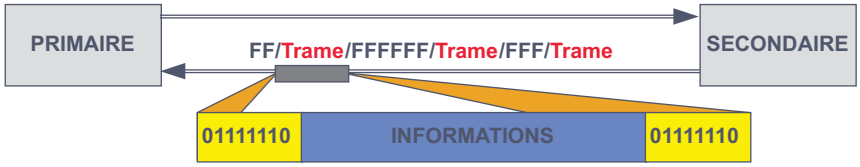


Figure 6.39 La liaison HDLC.

HDLC est un protocole qui utilise un mode de signalisation dans la bande. À cet effet, on distingue trois types de trames (figure 6.40).

Figure 6.40 Les fonctions et trames correspondantes d'HDLC.

Les trames d'information ou trames **I** assurent le transfert de données ; les trames de supervision ou trames **S** (*Supervisor*) le contrôlent (accusé de réception...), les trames non numérotées ou trames **U** (*Unnumbered*) supervisent la liaison. Les trames U sont des trames de signalisation.

© Dunod – La photocopie non autorisée est un délit

6.5.2 Structure de la trame HDLC

Le type de la trame émise (information, supervision ou contrôle de liaison) n'est pas distingué par un caractère particulier mais par une combinaison de bit (**protocole orienté bit**) Ce champ de bit est dit champ de commande ou de contrôle. La structure de la trame est donnée par la figure 6.41.

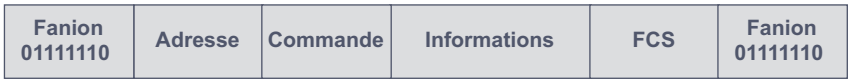


Figure 6.41 Structure générale de la trame.

La structure générale de la trame résulte de l'utilisation première d'HDLC. Contrairement à la structure classique « adresse source/adresse destination », la trame HDLC ne comporte qu'un seul champ d'adresse. Utilisé à l'origine dans une relation maître/esclave, un seul champ d'adresse était alors nécessaire. Il désignait le terminal auquel on transmettait des données, ou le terminal qui transmettait des données. L'échange ne pouvant avoir lieu qu'entre un terminal (esclave) et la machine maître, il n'y avait aucune nécessité d'un second champ d'adresse.

Le fanion, constitué de 8 éléments binaires (01111110), délimite la trame : fanion de tête et fanion de queue. Le fanion de queue pouvant faire office de fanion de tête de la trame suivante. La transparence est réalisée selon la technique dite du **bit de bourrage**.

Le champ commande, 8 ou 16 bits selon que les compteurs de trames sont sur 3 ou 7 bits, identifie le type de trame. Le paragraphe suivant détaille et explique les différentes fonctions de ce champ. Le champ informations est facultatif, il contient les informations transmises.

Enfin, le champ **FCS** ou *Frame Check Sequence*, champ de contrôle d'erreur, contient sur deux octets le reste de la division polynomiale (CRC) du message transmis (Adresse, Commande, Informations) par le polynôme générateur $x^{16} + x^{12} + x^5 + 1$. Le CRC, calculé à l'émission, est vérifié à la réception.

6.5.3 Les différentes fonctions de la trame HDLC

Le protocole HDLC distingue trois types de trames, identifiés par le champ de commande. La structure et la signification des sous-champs du champ de commande sont données par la figure 6.42.

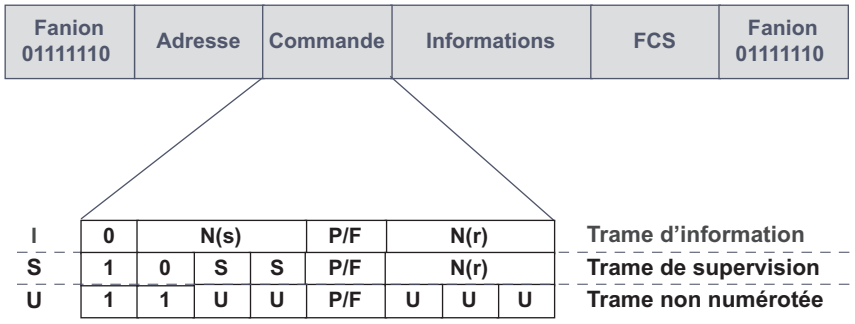


Figure 6.42 Structure du champ de commande.

Les trames d'information (I) contiennent un champ de données. Les champs notés N(s), N(r) correspondent, pour chaque extrémité de la liaison, à un compteur de trames d'information émises N(s) ou reçues N(r). Les trames de supervision (S) permettent de superviser l'échange de données. Le champ N(r) permet d'identifier la trame acceptée ou refusée. Les bits S identifient la commande. Les trames non numérotées (U, *Unnumbered*) gèrent la liaison (établissement, libération...). Elles ne comportent aucun compteur (non numérotées). Les bits S et U identifient la commande.

Le champ de commande comporte 3 champs :

– Un champ binaire qui identifie le type de trame (I, S, U) et la commande.

– Un bit de contrôle de la liaison P/F. Ce bit est positionné à 1 par le primaire lorsque celui-ci sollicite une réponse du secondaire (P = 1 pour *Poll sollicitation*). Le secondaire répond avec F = 1 (*Final*) à la sollicitation du primaire. C'est le cas, par exemple, en fin de fenêtre (figure 6.43), le bit P = 1 oblige le correspondant à répondre. Le secondaire répond par un acquittement avec F = 1, ou avec des trames d'information avec F = 0, sauf pour la dernière (F = 1).

– Des champs compteurs N(s), N(r) ; chaque station maintient à jour deux compteurs, un compteur de trames émises, N(s) variant de 0 à N ; un compteur de trames reçues N(r) variant de 1 à $N + 1$. Le champ N(s) est utilisé pour la numérotation des trames émises, alors que N(r) sert à l'acquittement, il contient le numéro de la prochaine trame attendue : N(r) = x acquitte les (x – 1) trames précédentes.

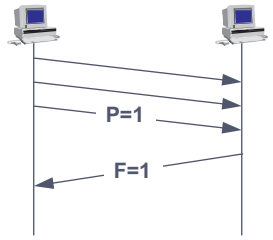


Figure 6.43 Utilisation du bit P/F.

La figure 6.44 détaille les principales commandes utilisées et précise les combinaisons de bits correspondantes.

Les modes de fonctionnement dépendent de deux données : la taille du champ de commande et la capacité d'initiative des stations secondaires. Le mode standard est caractérisé par un champ de commande sur 8 bits. La numérotation des trames sur 3 bits autorise une fenêtre théorique de 8 trames, en pratique 7. Le mode étendu possède un champ de commande sur 16 bits, la numérotation des trames est sur 7 bits, ce qui porte la limite de la fenêtre à 128 trames, en pratique 127. Ce dernier mode est utilisé dans les réseaux locaux (taux d'erreur faible) et dans les liaisons satellites (temps de transit important).

La capacité d'initiative des stations caractérise 2 modes : le mode normal et le mode asynchrone. Dans le mode *Normal Response Mode* (**NRM**), la commande est centralisée, les stations n'ont aucune initiative (relation maître/esclave). Le mode asynchrone peut être dissymétrique (**ARM**, le secondaire peut émettre sans invitation) ou symétrique (**ABM**, chaque extrémité est primaire en émission et secondaire en réception).

© Dunod – La photocopie non autorisée est un délit

Format	Commandes	Réponses	Hex*.	Champ Commande				
				8 7 6	5	4 3 2		1
I	INFORMATION		xx	N(r)	P/F	N(s)		0
S	RR		x1	N(r)	P/F	0 0	0	1
	RNR		x5	N(r)	P/F	0 1	0	1
	REJ		x9	N(r)	P/F	1 0	0	1
U	SABM		2F/3F	0 0 1	P	1 1	1	1
	SABME		6F/7F	0 1 1	P	1 1	1	1
	DISC		43/53	0 1 0	P	0 0	1	1
		UA	63/73	0 1 1	F	0 0	1	1
		FRMR	87/97	1 0 0	F	0 1	1	1
		DM	0F/1F	0 0 0	F	1 1	1	1

* les valeurs, exprimées en hexadécimal, dépendent de la position du bit P/F

I	**I**nformation	Trame d'information.
RR	**R**eceive **R**eady	Prêt à recevoir, accusé de réception utilisé lorsque le récepteur n'a pas de trame d'information à envoyer.
RNR	**R**eceive **N**ot **R**eady	Non prêt à recevoir, le récepteur demande à l'émetteur d'arrêter ses émissions, et acquitte les trames acceptées N(r) –1.
REJ	**Rej**ect	Rejet, demande de retransmission à partir de la trame N(r).
DISC	**DISC**onnect	L'un des ETTD prend l'initiative de la rupture de connexion.
SABM	**S**et **A**synchronous **B**alanced **M**ode	Commande permettant le passage en mode équilibré, il n'y a pas de notion de primaire et de secondaire. Chaque station peut émettre sans autorisation.
SABME	**S**et **A**synchronous **B**alanced **M**ode	Commande identique à la précédente, mais passage en mode étendu (numérotation modulo 128).
UA	**U**nnumbered **A**cknowledge	Acquitte une trame non numérotée.
FRMR	**Fram**e **R**eject	Informe de la réception d'une trame qui n'a pu être acceptée.
DM	**D**isconnect **M**ode	Indique que la station est déconnectée.

Figure 6.44 Les principales commandes d'HDLC.

6.5.4 Fonctionnement d'HDLC

Établissement et rupture de connexion

La liaison étant dans l'état logique déconnecté (figure 6.45), le primaire demande l'établissement d'une liaison par l'envoi de trames non numérotées (U) de type SABM (mode équilibré ou LAP-B, *Link Access Protocol Balanced*) ou SARM (mode maître/esclave ou LAP), le bit P est positionné à 1 (il aurait pu être à 0). Le secondaire, s'il accepte la connexion, répond par la trame non numérotée UA, le positionnement du bit F, dans la réponse, est identique à celui du bit P. La liaison est établie, l'échange d'informations peut alors commencer.

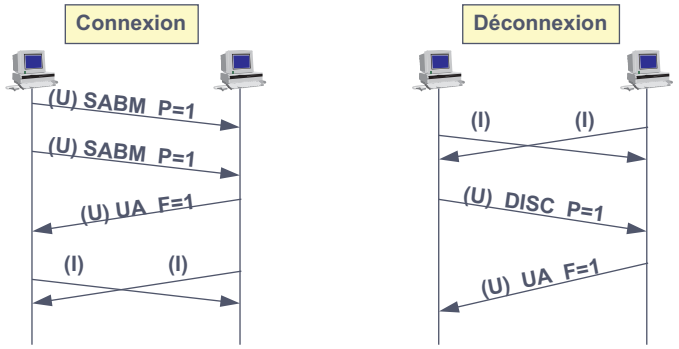


Figure 6.45 Gestion de la connexion sous HDLC.

La liaison est dans l'état logique connecté. Le primaire émet une demande de déconnexion DISC (figure 6.45), le bit P est positionné indifféremment à 1 ou à 0. Le secondaire accuse réception avec UA, la valeur du bit F correspond à celle du bit P de la trame DISC. La liaison est rompue. L'échange de fanions se poursuit pour maintenir la synchronisation tant que la liaison physique n'est pas rompue.

L'échange des données

La figure 6.46 illustre les différentes étapes d'un échange HDLC. Chaque entité correspondante entretient 2 compteurs dits **variables d'état**, le compteur V(s) indique le numéro de la prochaine trame à émettre, le compteur V(r) le numéro de la trame attendue. Après la phase de connexion les compteurs sont initialisés à zéro de chaque côté, la fenêtre étant de 7 (dans cet exemple), chaque entité a un crédit d'émission de 7 (ligne 1). En ligne 2, la machine A émet une trame, les compteurs N(s) et N(r) contiennent respectivement les valeurs V(s) et V(r) de la ligne 1. Les valeurs V(s), V(r) et crédit de la ligne 2 correspondent aux valeurs, mises à jour après émission de la trame pour la machine A et après sa réception pour la machine B. C'est-à-dire, que dans la figure, les valeurs des compteurs correspondent toujours aux valeurs mises à jour après réception ou émission d'une trame. Les lignes 3, 4, 5 n'appellent aucun commentaire particulier. En ligne 6, la machine B émet une trame. Son compteur Vr contient la valeur de la trame attendue, ici 4, il correspond pour la machine B à un acquittement des [N(s) – 1] trames émises, soit ici les trames 0, 1, 2 et 3. Les mémoires tampons sont libérées, la fenêtre est réinitialisée (crédit de 7).

Cette technique d'acquittement simultané à l'envoi de données, dite du *piggybacking*, optimise l'échange de données et évite un blocage de la fenêtre.

© Dunod – La photocopie non autorisée est un délit

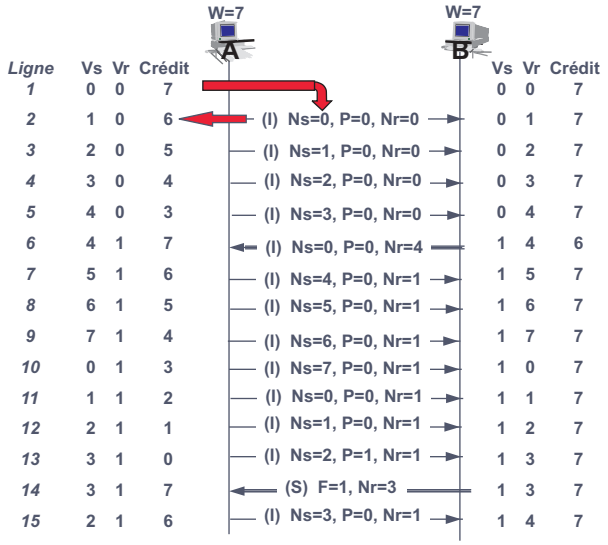


Figure 6.46 L'échange de données et la gestion de la fenêtre.

L'échange se poursuit, la fenêtre de A s'incrémente. En ligne 12, le crédit n'est plus que d'une trame, il sera nul à l'émission de la trame suivante (ligne 13). La trame émise demande alors un acquittement à B. N'ayant pas de données à envoyer, B acquitte, les trames reçues, avec une trame de supervision RR (*Receive Ready*). Il indique à A que cette trame est la réponse à sa demande en positionnant le bit F à 1.

Gestion des temporisations

Deux temporisateurs (figure 6.47) sont gérés par les entités communicantes :

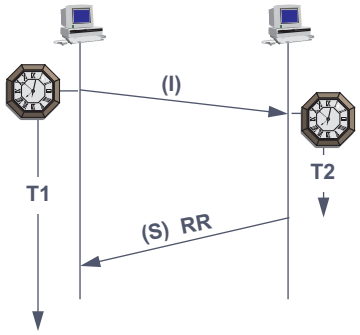


Figure 6.47 Gestion des temporisations.

– La **temporisation de retransmission** (**T1** ou **RTO**, *Retransmission Time Out*), à chaque trame émise l'émetteur initialise le temporisateur T1. Si, à l'échéance de ce temporisateur ou délai de garde, l'émetteur n'a pas reçu de trame d'information ou d'acquittement de son correspondant, il réémet la trame supposée perdue.

– La **temporisation d'acquittement** (**T2**) correspond au délai maximum au bout duquel, le récepteur, s'il n'a pas de données à transmettre, doit envoyer un acquittement à son correspondant.

Gestion des erreurs

La figure 6.48 illustre la reprise sur erreur. Supposons la trame 2 erronée, elle est ignorée par le récepteur. La trame 3 est alors reçue hors séquence, elle est rejetée. La machine B émet alors une trame de supervision de rejet (REJ, *Reject*) en indiquant à A à partir de quelle trame il doit reprendre la transmission [N(r) = 2]. Toutes les trames dont la valeur de Ns est supérieure à 2 sont alors rejetées (rejet simple).

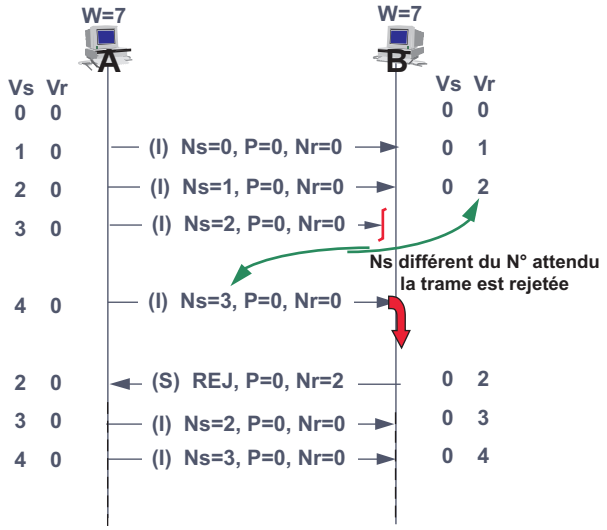


Figure 6.48 Gestion des erreurs.

La machine A reprend la transmission à partir de la trame 2 (Ns = 2). Si, suite à la trame erronée, A n'avait plus de données à émettre, B n'aurait pas détecté le déséquencement. C'est A qui, à l'échéance du temporisateur T1, aurait pris l'initiative de retransmettre la trame 2.

Gestion du contrôle de flux

HDLC utilise le contrôle de flux implicite. La fenêtre est paramétrée à l'installation du logiciel ou négociée lors de la connexion par le protocole de niveau supérieur. En cas de saturation des tampons de réception, le récepteur, ici dans la figure 6.49 la machine B, rejette la trame en excès et informe A de son incapacité temporaire à accepter de nouvelles données. Il émet la trame « S » **RNR** (*Receive Not Ready*) avec le compteur Nr positionné au numéro de la trame reçue et rejetée.

La machine A prend en compte cette demande et interroge (*poll*) régulièrement (tous les T1) la machine B, pour d'une part signaler sa présence et d'autre part formuler auprès de B une demande de reprise de transmission à l'aide de la trame « S » **RR**, *Receive Ready*, avec le bit P à 1.

Lorsque B peut reprendre la réception, il le signale à l'émetteur en accusant réception à l'aide de la trame « S » RR. Le compteur N(r) contient le numéro à partir duquel la retransmission doit reprendre. A avait positionné le bit P à 1, la réponse de B est émise avec le bit F à 1.

© Dunod – La photocopie non autorisée est un délit

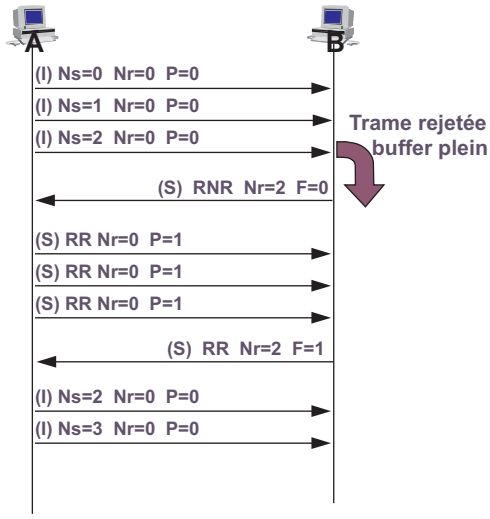


Figure 6.49 Gestion du contrôle de flux.

L'ambiguïté du bit P/F

Rappelons, qu'à l'origine HDLC était utilisé comme protocole de ligne dans les systèmes informatiques importants. Dans ces systèmes, c'est l'ordinateur central qui contrôle le dialogue (politique d'accès centralisée), la relation est dite maître/esclave. L'ordinateur interroge les terminaux (*polling*, P = 1), le terminal interrogé doit répondre, dans la dernière trame de sa réponse le bit F est mis à 1 (final). Ces appellations ont été conservées.

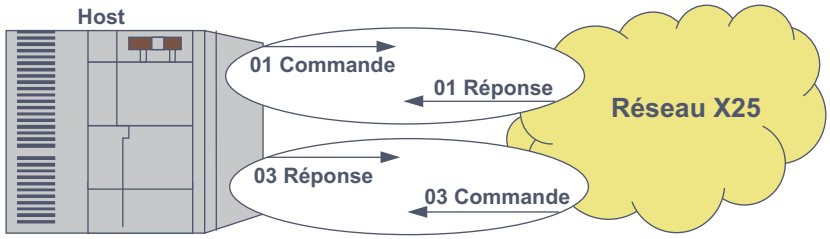


Figure 6.50 Gestion du bit P/F dans X.25.

En mode équilibré, chaque extrémité de la liaison peut, en positionnant le bit P à 1, prendre l'initiative de solliciter une réponse de l'autre extrémité. Si les deux entités formulent, en même temps, une demande de réponse, le protocole HDLC ne distinguant pas le bit P du bit F, chaque entité prend la demande de l'autre comme la réponse à sa propre demande (figure 6.50).

HDLC en mode équilibré est utilisé en protocole ligne, c'est-à-dire en liaison point à point : le champ adresse est inutile. Dans ces conditions, il est possible d'utiliser le champ adresse comme extension du champ de commande afin d'identifier le sens de la requête. Cette possibilité est utilisée pour contrôler le dialogue entre un réseau et son abonné (figure 6.50) :

– dans le sens Host/Réseau, le champ adresse contient la valeur binaire 01,

– dans le sens Réseau/Host, le champ adresse contient la valeur binaire 11.

6.5.5 Les différentes versions du protocole HDLC

Normalisé en 1976 (CCITT et ISO) HDLC a inspiré de nombreuses les variantes :

– mode **LAP** (*Link Access Protocol*), fonctionnement sur sollicitation du primaire ;

– mode **LAP**-B (B pour *Balanced*, mode équilibré), dans ce type de liaison, il n'y a pas de primaire prédéfini, chaque station peut être primaire ;

– mode **LAP-D** (D pour canal D), ce protocole similaire à LAP-B est utilisé dans les réseaux numériques (RNIS) ;

– mode **LAP-M** (M pour Modem), dérivé de LAP-D, il est mis en œuvre pour des connexions PC-Calculateur hôte, ce protocole est utilisé dans les modems conformes aux recommandations V.42 et V.42 bis ;

– mode **LAP-X**, mode semi-duplex dérivé de LAP-D, est utilisé dans le télétex.

Notons que **SDLC**, *Synchronous Data Link Control*, utilisé dans l'environnement **IBM SNA**, *System Network Architecture*, est parfois présenté comme un sous-ensemble d'HDLC car moins riche ; cependant, il est plus logique de présenter HDLC comme une évolution de SDLC. SDLC ne fonctionne qu'en mode non équilibré.

6.5.6 HDLC et les environnements multiprotocoles

Dans un contexte multiapplications, deux applications peuvent utiliser un protocole de communication X et un autre couple d'application un protocole Y (figure 6.51), Le transport des informations de chacune des liaisons applicatives ne peut être réalisé par HDLC. En effet, HDLC est certes un protocole de liaison de point à point, mais ne pouvant distinguer les données des protocoles X ou Y, HDLC ne peut être utilisé que dans un environnement monoprotocole.

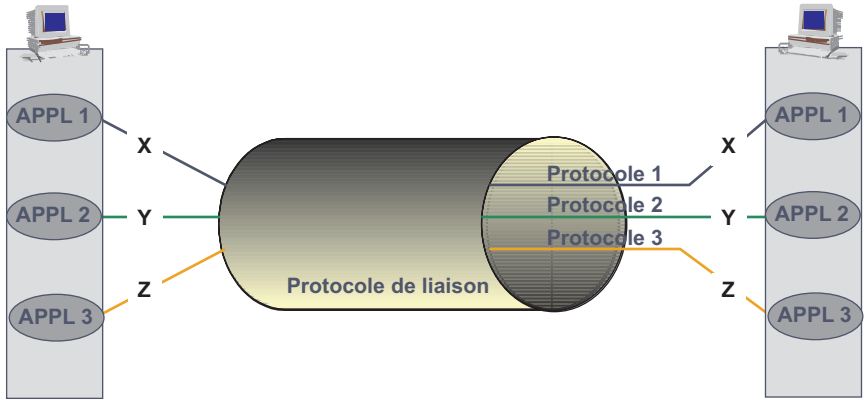


Figure 6.51 Liaison multiprotocoles.

Le protocole **PPP** (*Point to Point Protocol*), inspiré de HDLC remédie à cet inconvénient. À cet effet, un champ spécifique : Protocol_ID est inséré entre le champ commande et le champ données d'HDLC. PPP sera étudié au chapitre 10. Le format de trame représenté ci-dessous (figure 6.52) est dérivé de celui des trames UI (trame non numérotée d'HDLC), le champ adresse contient la valeur 0xFF et le champ commande 0x03 (trame UI), le champ

© Dunod – La photocopie non autorisée est un délit

Protocol_ID indique le protocole utilisé par les données transportées dans le champ données. On dit alors que le protocole X ou Y est encapsulé dans PPP.

Fanion	Adresse	Commande	Protocol_ID	Données	FCS	Fanion
01111110	11111111	00000011	1 ou 2 octets	0 à 1 500 octets	2 ou 4 octets	01111110

Figure 6.52 Trame PPP (format non numéroté).

6.6 CONCLUSION

HDLC, en version LAP-B, est utilisé dans les réseaux de type X.25 (exemple : Transpac). Les contrôles d'erreur et de flux sont effectués de point à point (nœud à nœud). Cette technique est efficace mais pénalise gravement les performances d'HDLC. L'évolution des techniques réseaux (fibres optiques) rend les supports plus fiables (taux d'erreur plus faible) et autorise une simplification des protocoles. En confiant aux calculateurs d'extrémité (ceux qui sont connectés au réseau), les tâches de contrôle d'erreur et de contrôle de flux, la technique du relais de trames (*Frame Relay* ou LAP-F) permet des débits effectifs plus élevés (34 368 kbit/s).

La réalisation de liaisons point à point entre les systèmes d'information peut se révéler coûteuse au regard du temps d'utilisation. Aussi, indépendamment de la notion de protocole ou d'environnement multiprotocoles, il peut paraître intéressant d'examiner si une liaison peut être utilisée simultanément par plusieurs entités communicantes. C'est la notion de « mutualisation » des ressources ou de concentration de trafic que nous allons aborder au prochain chapitre.

EXERCICES

Exercice 6.1 Calcul de CRC

Calculez le CRC4 pour les données 1010010111, le polynôme générateur étant $x^4 + x^2 + x + 1$.

Exercice 6.2 Probabilité de recevoir un message erroné

On définit le taux d'erreur binaire ou TEB (Te) comme le rapport du nombre de bits reçus en erreur au nombre total de bits reçus. Une transaction de 100 caractères ASCII est émise sur une liaison en mode synchrone à 4 800 bit/s avec un Te de 10^{-4}.

Les erreurs sont supposées être distribuées aléatoirement, c'est-à-dire que la probabilité d'avoir un bit en erreur est la même pour tous les bits, et est égale au Te. Déterminez la probabilité pour qu'un message reçu comporte au moins une erreur (Pe).

Exercice 6.3 Taux de transfert

Un fichier est transmis par blocs de 1 000 caractères codés en ASCII, avec 1 bit de parité, en mode synchrone sur une liaison à 9 600 bit/s. On suppose, en outre, que la transmission est effectuée en mode semi-duplex et la demande de retransmission instantanée. Calculez :

a) Le taux de transfert des informations (TTI) ou débit effectif ;

b) Le TTI avec erreur si on suppose un Te de 10^{-4}.

Exercice 6.4 Échange de trames HDLC version LAP-B

Le tableau ci-après (figure 6.53) représente les différentes étapes d'un échange LAP-B entre deux correspondants A et B. Il vous est demandé de le compléter. La colonne de droite vous indique l'action. Le « ? » signifie que c'est à vous d'indiquer l'action correspondante. Les valeurs des compteurs N(s) et N(r) indiquées dans les colonnes correspondent aux valeurs des variables d'état [V(s) et V(r)] mises à jour après l'action correspondante. La fenêtre est fixée à 4 dans les deux sens.

© Dunod – La photocopie non autorisée est un délit

	A			B	
Valeur des compteurs après l'échange après émission et après réception)	V(s)	V(r)	Échange	V(s)	V(r)
Exemples de trames : Indiquer le type (I, U, S) Éventuellement la trame (REJ, SABME...) Les valeurs des compteurs Nr, Ns La valeur du bit P/F			(I) Ns=4 Nr=6 P=0 ——————> (S) RNR Nr=3 P=0 <——————		
Initialisation :	0	0		0	0
1) Ouverture en mode asynchrone normal					
2) Acceptation par B					
Échange					
3) Trame d'information de A vers B					
4) Trame d'information de A vers B erronée					
5) Trame d'information de A vers B					
6) ?					
7) Trame d'information de A vers B					
8) Trame d'information de A vers B					
9) Trame d'information de B vers A					
10) Trame d'information de A vers B					
11) Trame d'information de A vers B					
12) Trame d'information de A vers B					
13) Trame d'information de A vers B					
14) ?					
Fermeture de la connexion					
15) Demande de fermeture					
16) Acquittement par B					

Figure 6.53 Échange LAP-B.

Chapitre **7**

La mutualisation des ressources

Lors de la réalisation d'une liaison de transmission de données, le responsable réseau et télécoms d'une entreprise se doit de rechercher la meilleure solution en termes d'efficacité et de coût. Cet objectif d'optimisation des moyens de transmission et des coûts se concrétise par la recherche :

– du meilleur dimensionnement des moyens (nombre de lignes, nombre de terminaux...) ;
– du meilleur taux de transfert, obtenu par une éventuelle réduction du volume à transmettre (compression de données) ;
– de l'utilisation de protocoles efficaces (évolution d'HDLC vers le **Frame Relay**)
– d'une solution de partage des moyens entre plusieurs utilisateurs (mutualisation des ressources), c'est la concentration de trafic.

La concentration de trafic n'est réalisable que si chacun des participants ne monopolise pas les ressources attribuées. La première étape de l'étude d'une solution de concentration consiste à évaluer le trafic de chacun en le quantifiant, puis à rechercher en fonction du type de relation à mettre en œuvre la meilleure solution.

7.1 LA QUANTIFICATION DE TRAFIC

7.1.1 Généralités

Prenons l'exemple d'une application de type conversationnel (échange questions/réponses entre un terminal et un ordinateur), si on examine le déroulement d'une session, limitée à un seul échange dans l'illustration de la figure 7.1, on constate que :

– la durée de la session est bornée dans le temps, le support libéré est alors utilisable par un autre utilisateur : c'est la **commutation** ;

– pendant la durée de la session le support n'est pas en permanence utilisé pour la transmission de données. Durant les instants de silence, le support est disponible pour un autre utilisateur ou une session différente : c'est la **concentration de trafic**.

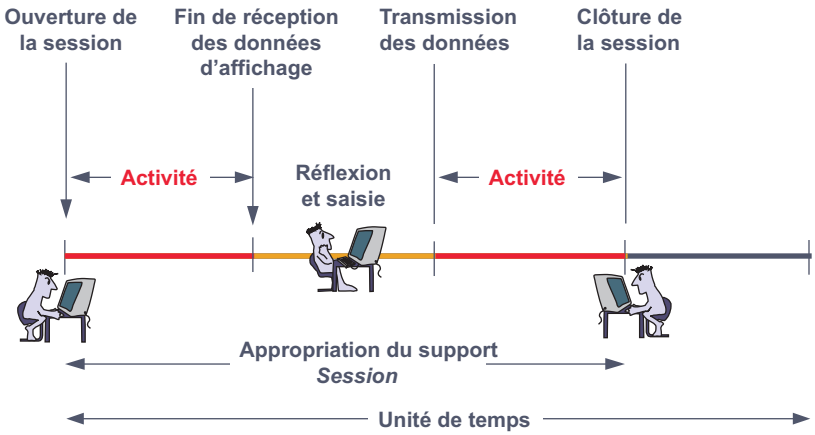


Figure 7.1 L'activité sur une ligne n'est pas permanente.

7.1.2 Intensité de trafic et taux d'activité

Évaluation des grandeurs

Deux grandeurs permettent de quantifier le trafic (figure 7.2) :

– l'intensité de trafic qui mesure la durée de la session ;

– le taux d'activité qui mesure l'utilisation effective du support.

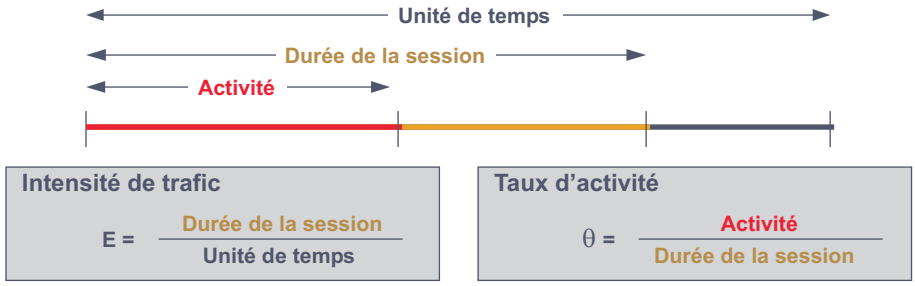

Unité de temps
Durée de la session
Activité
Intensité de trafic
E = Durée de la session / Unité de temps
Taux d'activité
θ = Activité / Durée de la session

Figure 7.2 Intensité de trafic et taux d'activité.

Intensité de trafic et dimensionnement des ressources

Lorsqu'un service est fourni à plusieurs utilisateurs et que ceux-ci ne l'utilisent pas en permanence, la question du dimensionnement des moyens d'accès se pose. C'est, par exemple, le cas des accès à Internet, le fournisseur d'accès (**ISP**, *Internet Service Provider*) doit déterminer le nombre de lignes et de modems qu'il doit mettre en ligne (figure 7.3).

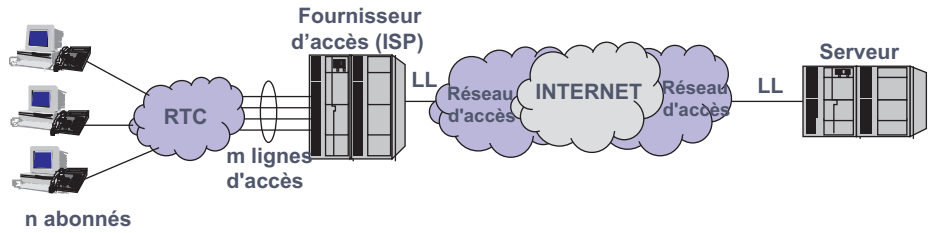


Figure 7.3 Détermination du nombre de lignes.

S'il dispose d'autant de lignes (m) que d'abonnés (n) aucun problème d'exploitation ne se présentera, mais il y aura vraisemblablement un « gâchis » de ressources. Si le nombre de lignes m est petit devant n, il y aura un taux de refus de mise en relation important. Le problème consiste donc à déterminer la valeur optimale du nombre de lignes nécessaires m pour que les abonnés aient une qualité de service acceptable (taux de refus faible et prédéterminé).

La relation entre intensité de trafic et ressources nécessaires a été étudiée par Erlang (mathématicien danois). Le dimensionnement des ressources nécessite de quantifier le trafic à écouler (Intensité de trafic), puis en fonction d'un taux de refus prédéterminé (probabilité que toutes les ressources soient utilisées quand l'utilisateur $n + 1$ désire se connecter) à définir le nombre de lignes m nécessaires.

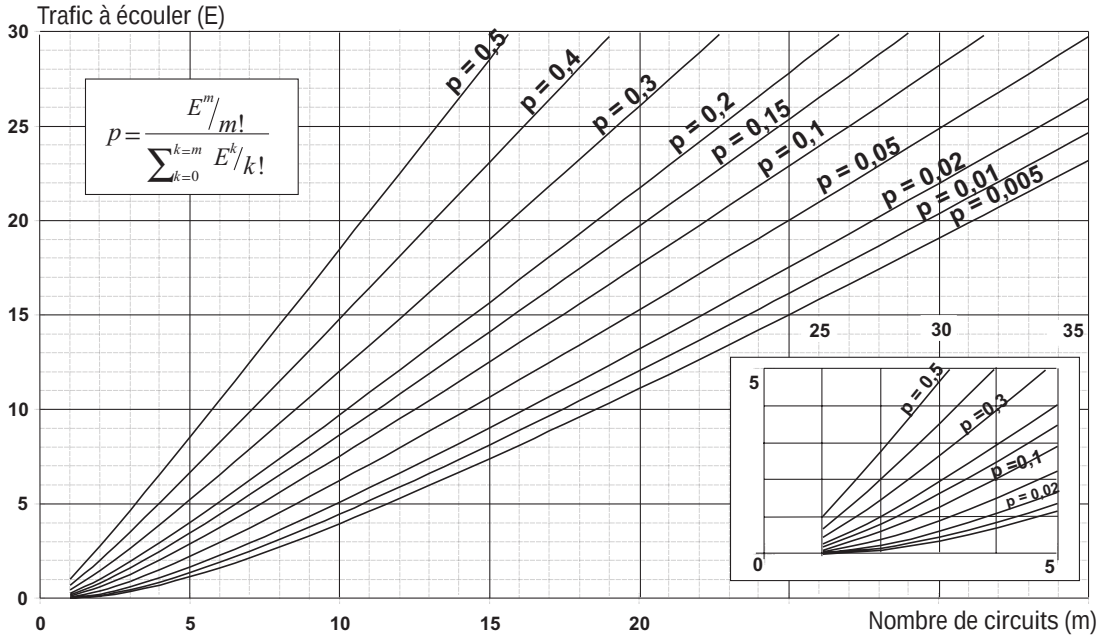


Figure 7.4 Abaque d'Erlang dit à refus.

Ce problème peut être résolu par l'utilisation de tables dites **tables d'Erlang** ou dites d'abaques d'Erlang. La figure 7.4 représente un abaque d'Erlang. Connaissant le trafic (E), la probabilité de refus (ou taux de blocage) choisie (p), il est possible de déterminer le nombre de lignes (m).

© Dunod – La photocopie non autorisée est un délit

Taux d'activité et concentration de trafic

Lorsque la somme des activités (θ) de plusieurs utilisateurs est inférieure à 1, la rationalisation de l'utilisation des moyens conduit à envisager de leur faire partager un même support :

$$\sum_{i=1}^{i=n} \theta_i \leqslant 1$$

C'est la notion de concentration de trafic illustrée par la figure 7.5.

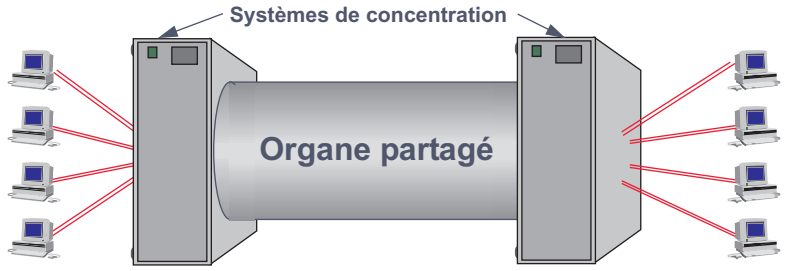


Figure 7.5 Principe de la concentration de trafic.

Selon la relation établie entre les *n* utilisateurs de l'organe partagé, on distingue (figure 7.6) :

- ceux qui permettent de relier *n* utilisateurs à un seul système (relation de *1 à n* et de *n à 1*), ce sont les *concentrateurs* ;
- ceux qui n'autorisent qu'une relation de *1 à 1*, ce sont les *multiplexeurs* ;
- enfin, ceux qui permettent une relation de *1 à 1* parmi *n* et de *1 à n* ce sont les *réseaux*. Les réseaux feront l'objet d'une étude détaillée au chapitre suivant.

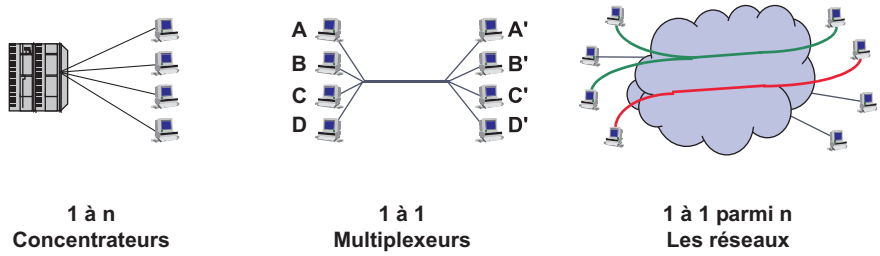


Figure 7.6 Les différents organes de concentration.

7.2 LES CONCENTRATEURS

7.2.1 Principe

Les concentrateurs sont essentiellement utilisés en informatique traditionnelle. Il autorise l'utilisation d'une seule liaison pour l'accès de *n* terminaux à l'ordinateur central (figure 7.7). Le concentrateur analyse le contenu des blocs d'information reçus et les dirige vers le seul terminal concerné. De ce fait, le concentrateur n'est pas transparent aux protocoles : il doit être

capable d'analyser les données qu'il transmet. Il dispose, pour cela, d'une logique programmée.

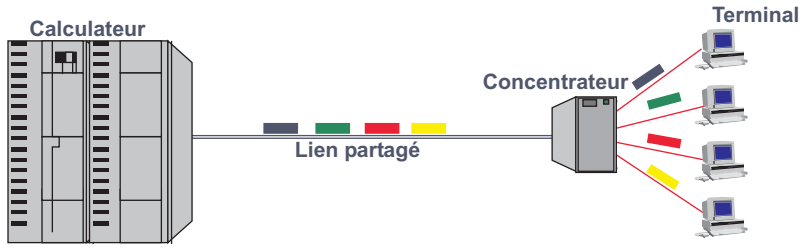


Figure 7.7 Principe de la concentration de terminaux.

Avec le développement des réseaux locaux, le concentrateur en tant que tel tend à disparaître. Un micro-ordinateur, désigné sous le terme de passerelle, assure la fonction de concentration. Un logiciel spécifique, chargé sur un micro-ordinateur, poste de travail, émule le terminal passif traditionnel. Cette utilisation est illustrée par la figure 7.8.

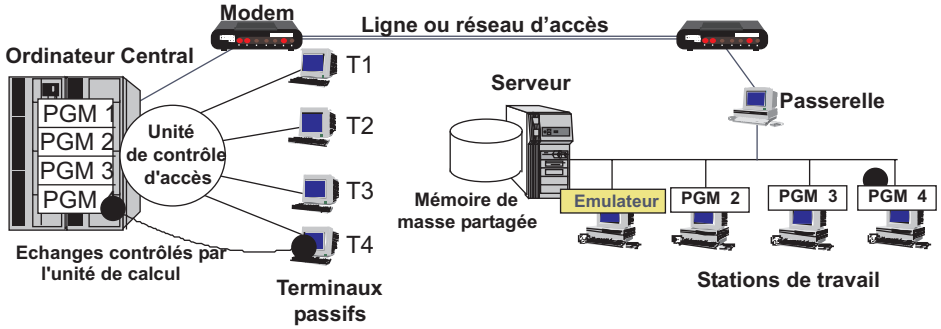


Figure 7.8 L'accès aux ordinateurs centraux via un réseau local.

7.2.2 Fonctionnalités complémentaires, exemple d'application

Le concentrateur, lorsqu'il reçoit un message l'analyse, interprète les données d'aiguillage et retransmet vers le destinataire les informations reçues en effectuant, éventuellement, une conversion de protocole. C'est le cas notamment des points d'accès vidéotex (**PAVI** figure 7.9).

Le PAVI est un concentrateur qui, outre les fonctions de concentration, assure :

– La conversion de protocole, les caractères reçus, en mode asynchrone en provenance du terminal Minitel (terminal asynchrone) sont regroupés en blocs de données (paquets) et émis en mode synchrone selon le protocole X.25[1] sur le réseau Transpac. De manière inverse, les données reçues sous forme de paquets par le PAVI, en provenance de l'ordinateur serveur, via le réseau X.25, sont désassemblées et transmises caractère par caractère au terminal Minitel (fonction **PAD**, *Packet Assembler Dissassembler*). Ce procédé évite que sur le réseau X.25 on ne fasse 1 caractère = 1 paquet.

1. Le protocole X.25 est étudié à la section 11.2.2. La société Transpac a mis en service en 1978 le premier réseau public de transmission en mode paquets X.25.

© Dunod – La photocopie non autorisée est un délit

– La conversion de débit entre le terminal Minitel et le réseau X.25.
– L'écho distant du caractère, un terminal asynchrone n'affiche pas le caractère frappé sur le clavier mais celui reçu en écho de la machine hôte distante. Pour ne pas surcharger le réseau, c'est le PAVI qui assure l'écho de caractère.

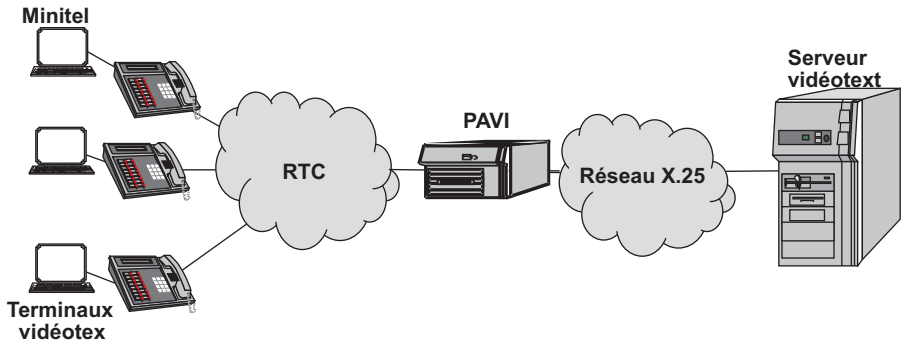


Figure 7.9 Une concentration particulière : l'accès vidéotex.

Ainsi, un concentrateur peut assurer :
– l'écho de caractère (terminal asynchrone) ;
– le contrôle de la validité des informations ;
– la mise en forme des données ;
– la mémorisation des informations reçues (gestion de files d'attente) ;
– la gestion des terminaux (contrôleur d'écran, polling...).

7.3 LES MULTIPLEXEURS

7.3.1 Principe

Le multiplexeur est un équipement qui met en relation un utilisateur avec un autre par l'intermédiaire d'un support partagé par plusieurs utilisateurs. Un multiplexeur *n* voies simule, sur une seule ligne, *n* liaisons point à point. Chaque voie d'entrée est dénommée voie incidente, le support partagé voie composite (figure 7.10).

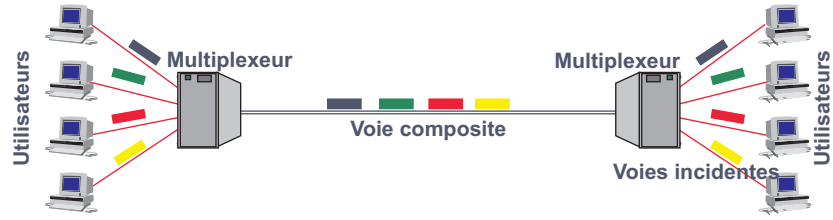


Figure 7.10 Principe du multiplexage.

L'opération de regroupement des voies incidentes sur un même support s'appelle le multiplexage. Le démultiplexage consiste à restituer à chaque destinataire les données des diffé-

rentes voies. La figure 7.11 représente une liaison par multiplexeur. Un multiplexeur est un système symétrique, un MUX (abréviation utilisée pour désigner un multiplexeur) comporte à la fois un organe de multiplexage et un organe de démultiplexage (liaison *full duplex*).

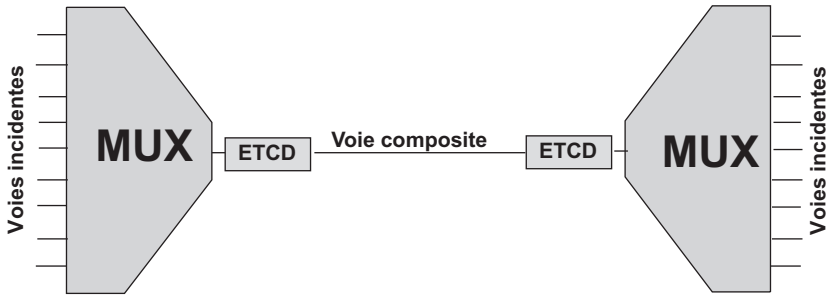


Figure 7.11 Représentation symbolique d'une liaison multiplexée.

Le partage de la voie composite peut être un partage :

– de la bande disponible, chaque voie dispose en permanence d'une fraction de la bande disponible, c'est le **multiplexage fréquentiel** ou **spatial** ;
– du temps d'utilisation de la voie, chaque voie utilise durant un temps prédéterminé toute la bande disponible, c'est le **multiplexage temporel**.

7.3.2 Le multiplexage spatial

Le multiplexage fréquentiel (**FDM**, *Frequency Division Multiplexing*) correspond à une juxtaposition fréquentielle de voies et à une superposition des signaux dans le temps. La bande passante du support est divisée en canaux (voies). Chaque voie est modulée (transposition de fréquence) par une porteuse différente, le démultiplexage correspond à l'extraction de chacune des voies (voies spatiales) par l'intermédiaire de filtres puis à la démodulation de chaque signal. La figure 7.12 illustre le principe d'un multiplexeur fréquentiel.

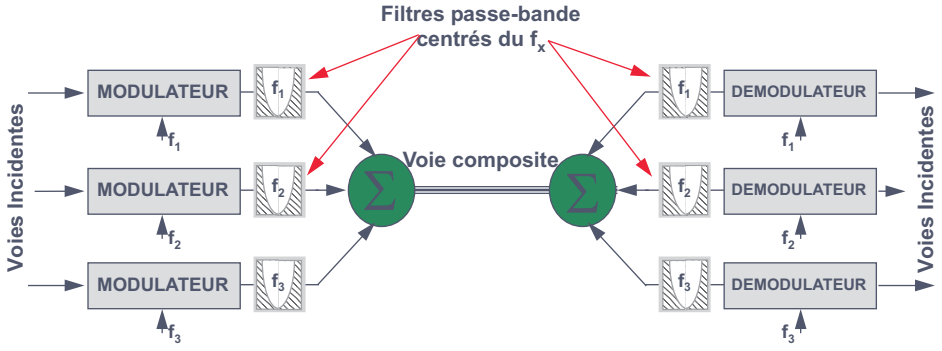


Figure 7.12 Principe du multiplexage fréquentiel.

Entre chaque voie ou canal, un espace de fréquence, dit **bande de garde**, sépare les canaux et évite l'intermodulation (figure 7.13), de plus, chaque voie dispose en permanence de la ressource qui lui est affectée, si un utilisateur n'utilise pas son canal, la bande correspondante est perdue. L'efficacité d'un tel système reste faible (0,2 à 0,3).

© Dunod – La photocopie non autorisée est un délit

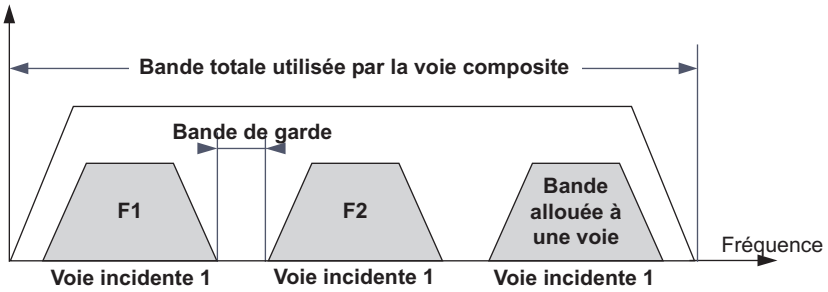


Figure 7.13 Partage de fréquence par les différentes voies.

Avant l'apparition des techniques de numérisation, le multiplexage fréquentiel a été utilisé pour constituer les premiers réseaux de téléphonie. L'unité de base ou voie basse vitesse a une largeur de bande de 4 kHz. Les voies basse vitesse sont multiplexées pour former un groupe de voies dit groupe primaire, ce dernier est lui-même multiplexé pour former un groupe secondaire... Ces regroupements ont formé la hiérarchie analogique comme indiquée dans le tableau de la figure 7.14.

Groupe	Bandes de fréquences	Nombre de voies téléphoniques
Primaire	60 à 108 kHz	12
Secondaire	312 à 552 kHz	60
Tertiaire	812 à 2 044 kHz	300
Quaternaire	8 516 à 12 388 kHz	900

Figure 7.14 La hiérarchie analogique.

Les liaisons optiques mettent en œuvre un cas particulier du multiplexage fréquentiel (figure 7.15) : le multiplexage de longueur d'onde (**WDM**, *Wavelength Division Multiplexing*). À l'origine seules, les fenêtres courantes de 1300 et 1550 nm ont été utilisées. Rapidement l'exploitation de 4 longueurs d'ondes dans la fenêtre de 1 530 à 1 560 nm (bande C) a permis la réalisation de liaisons à 10 Gbit/s (4 canaux de 2,5 Gbit/s) sur une distance de 250 km. Cette technique est limitée par la dispersion chromatique (différence de coefficient de vélocité en fonction de la longueur d'onde).

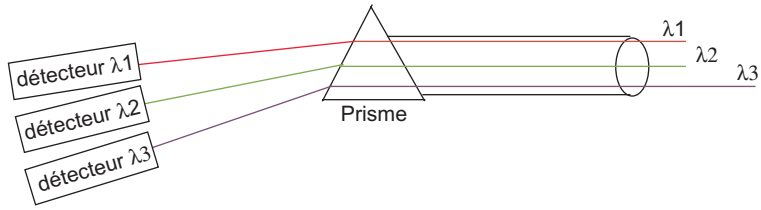


Figure 7.15 Principe du multiplexage de longueur d'onde.

Les technologies de *Dense WDM* (**DWDM**) ont permis la multiplication des canaux par réduction de l'écartement entre les canaux utilisés, de 1,6 nm à 0,2 nm. Aujourd'hui, on a pu réaliser des liaisons à 3 Tbit/s sur 7 300 km en utilisant 300 canaux à 10 Gbit/s et en laboratoire 10 Tbit/s sur 100 km avec 256 canaux à 40 Gbit/s.

7.3.3 Le multiplexage temporel

Principe

Quand le taux d'activité est inférieur à 1, entre deux épisodes de transfert, il existe des espaces de temps (silences) qui peuvent être utilisés par d'autres utilisateurs. Les multiplexeurs temporels relient une voie incidente d'entrée à une voie incidente de sortie durant un intervalle de temps prédéterminé. Cet intervalle de temps ou **IT**, réservé à un couple émetteur/récepteur, constitue une voie temporelle (figure 7.16).

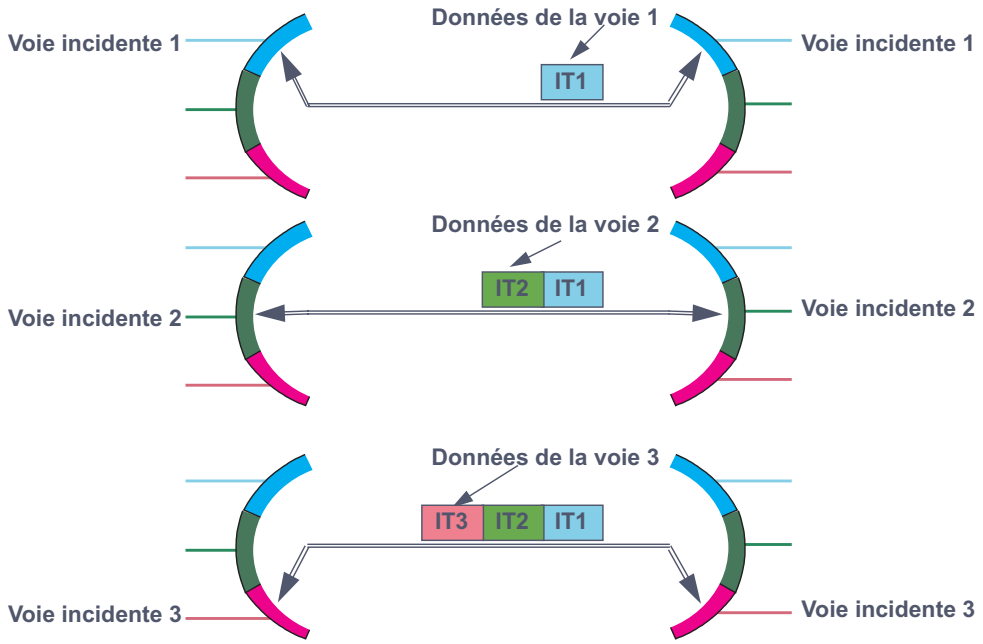


Figure 7.16 Principe du multiplexage temporel.

Dans le premier schéma de la figure 7.16, le couple de multiplexeurs met en relation les utilisateurs raccordés aux voies identifiées « voies incidentes 1 » ; l'intervalle de temps suivant, les utilisateurs raccordés aux voies 2, puis ceux raccordés aux voies 3. La restitution des différentes voies nécessite l'identification de celles-ci. Dans le système décrit, chaque voie est toujours scrutée à période constante, à chaque IT est donc associé une position dans la trame, c'est le multiplexage de position. Un IT de synchronisation permet d'identifier le début de trame, il assure le cadrage de la lecture des différentes voies (figure 7.17). L'ensemble des différentes voies et de (ou des) l'IT de synchronisation forme la trame multiplexée, couramment appelée le **multiplex**.

Un tel système transporte des bits, le multiplexeur n'interprète pas les données qu'il transporte, il est dit transparent au protocole. L'arrivée des données est indépendante du fonctionnement du multiplexeur. Les informations qui arrivent pendant la période de scrutation des autres voies incidentes sont mémorisées. Les multiplexeurs nécessitent de la mémoire et introduisent un retard de transmission qui peut être important vis-à-vis du temps de transfert sur le support.

© Dunod – La photocopie non autorisée est un délit

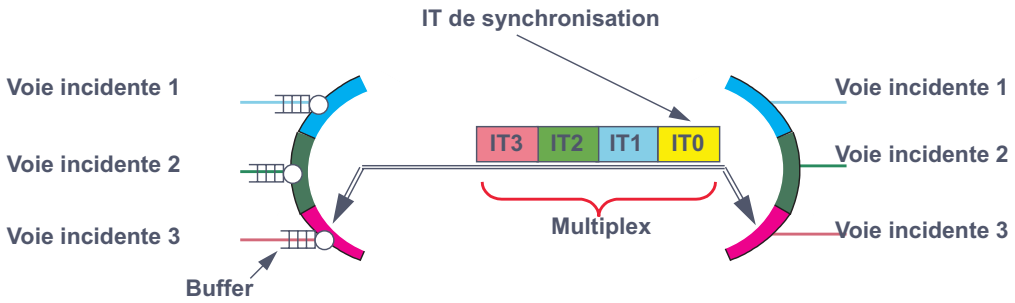


Figure 7.17 Structure élémentaire d'un multiplexeur.

Le multiplexage est dit caractère quand chaque IT est égal à un caractère. Dans un tel système, l'efficacité peut atteindre 0,8. Si on diminue encore le temps affecté, à un IT, jusqu'au niveau bit (1 IT = 1 temps bit), l'efficacité peut atteindre 0,9.

Notion de débit de cadrage

Dans un système de transmission chaque source est indépendante. Même, si on réalise à partir d'une horloge unique une distribution d'horloge, il est pratiquement impossible de garantir que les horloges de chaque système soient identiques (figure 7.18).

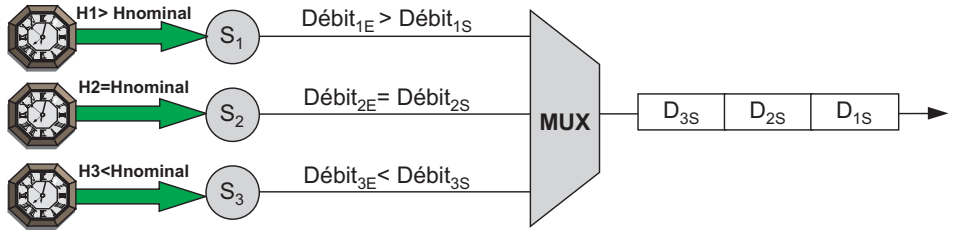


Figure 7.18 Distribution des horloges dans un réseau.

Le décalage des horloges provoque des inégalités de débit. Afin d'assurer l'égalité entre le débit incident et le débit correspondant sur le multiplex, il est nécessaire de prévoir, dans le multiplex de sortie, un surdébit pour permettre le cadrage des données (surdébit de cadrage). La figure 7.19 illustre le principe du mécanisme d'ajustement des débits par bit de cadrage.

Trame PDH		C_1	C_2	J_1	J_2	**Données**
Justification négative	$DS_1 < DE_1$	0	0	0	0	**Données**
Pas de justification	$DS_2 = DE_2$	0	1	0		**Données**
Justification positive	$DS_3 > DE_3$	1	1			**Données**

Figure 7.19 Principe de la justification dans les trames PDH.

Dans cet exemple, l'écart maximal des horloges a été fixé à 1 bit. La position des données dans la trame varie donc de ± 1 bit, par rapport à une position de référence (pas de justification). Les bits C_1 et C_2 indiquent lorsqu'ils sont positionnés à 1 que le bit de justification correspondant (C_1 pour J_1 et C_2 pour J_2) contiennent des données. Les bits de justification J_1 et J_2, lorsqu'ils ne sont pas utilisés, sont à zéro.

Les multiplexeurs statistiques

Bien que l'efficacité des multiplexeurs temporels soit nettement supérieure à celle des multiplexeurs spatiaux, l'utilisation de la ligne n'est pas optimale. En effet, la plupart des applications n'accèdent pas en permanence au support, de ce fait, il existe des temps morts où la ligne est inexploitée. Pour améliorer l'utilisation du support, les multiplexeurs statistiques allouent dynamiquement la bande disponible.

Les intervalles de temps sont alloués en fonction des besoins respectifs des voies incidentes. Les multiplexeurs statistiques nécessitent des mémoires tampons importantes pour stocker les données en attente d'émission.

Multiplexage de position et multiplexage d'étiquette

Dans le multiplexage de position, le débit de la source et celui du multiplex sont liés, le mode de transfert est dit synchrone (**STM**, *Synchronous Transfer Mode*). La bande non utilisée est perdue. Une bonne rentabilisation du système exigerait qu'il y ait décorrélation entre la bande utilisée par une voie et celle offerte par le système, c'est le mode de transfert asynchrone (**ATM**[2], *Asynchronous Transfer Mode*) qui caractérise les réseaux en mode paquets[3].

Dans ces réseaux les données sont émises au rythme de la source, elles ne peuvent plus être repérées par leur position. Elles sont alors identifiées par un label ou étiquette. On parle alors de **multiplexage d'étiquette**.

Le multiplexage inverse

Le multiplexage inverse (**IM**, *Inverse Multiplexing*) consiste en l'agrégation de plusieurs liens bas débit pour obtenir un débit, vu de l'utilisateur, égal à la somme des débits des liens agrégés (figure 7.20). Cette pratique permet d'améliorer la granularité de l'offre des opérateurs.

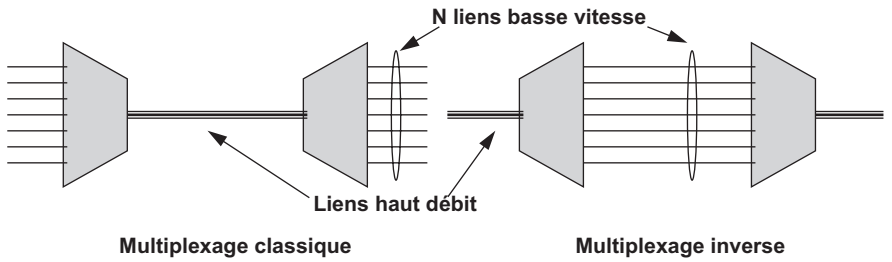


Figure 7.20 Principe du multiplexage inverse.

2. Il ne faut pas confondre le mode de transfert décrit avec le protocole du même nom qui n'est qu'un cas particulier du mode de transfert asynchrone (voir chapitre 11).
3. Les réseaux en mode paquets feront l'objet de l'étude du chapitre suivant.

© Dunod – La photocopie non autorisée est un délit

Exemple d'application : la trame MIC

➤ Principe

La numérisation de la voix autorise le multiplexage temporel de plusieurs communications téléphoniques (figure 7.21). La trame **MIC** (Modulation par Impulsion et Codage) regroupe 30 communications téléphoniques dans une même trame communément appelée E1, pour multiplex Européen d'ordre 1.

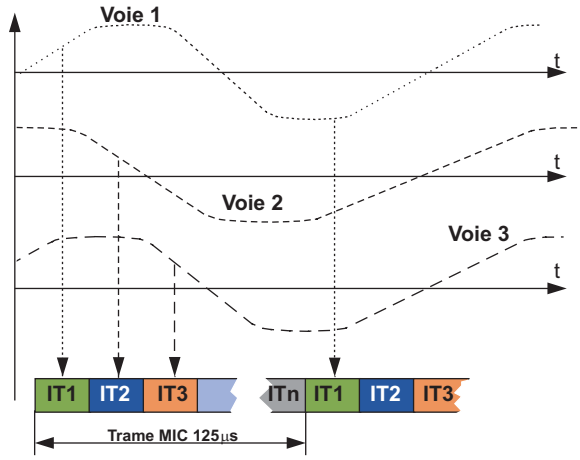


Figure 7.21 Principe de la trame MIC.

➤ Organisation de la trame

La trame MIC multiplexe 30 voies téléphoniques dans un conduit de 2 048 kbit/s, correspondant à un multiplex de 32 voies de 64 kbit/s. L'IT0 ou Mot de Verrouillage Trame (**MVT**) permet le repérage des IT dans les trames. L'IT16 de la trame 0 contient les informations de supervision de la trame et de cadrage pour les multiplex d'ordre supérieur. L'IT16 des autres trames transporte la signalisation des communications (informations sur l'état du canal). La figure 7.22 représente la trame MIC Européenne, les USA et le Japon ont adopté une structure différente.

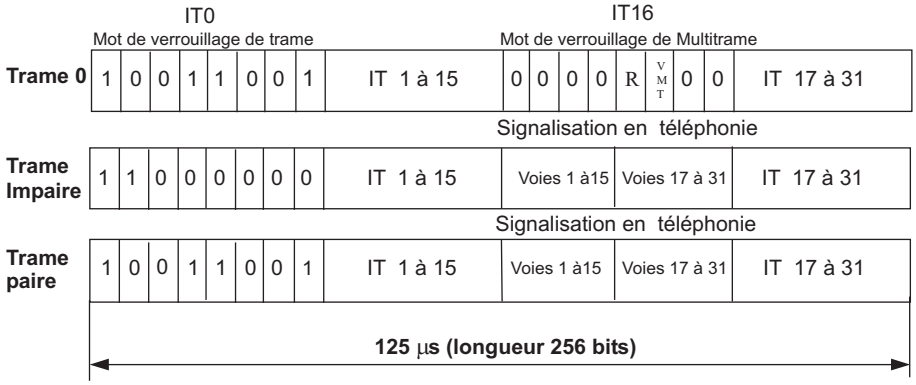
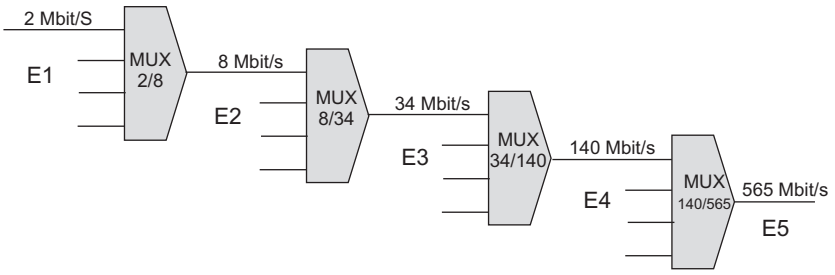

IT0
Mot de verrouillage de trame
IT16
Mot de verrouillage de Multitrame
Trame 0
1 0 0 1 1 0 0 1
IT 1 à 15
0 0 0 0 R V M T 0 0
IT 17 à 31
Signalisation en téléphonie
Trame Impaire
1 1 0 0 0 0 0 0
IT 1 à 15
Voies 1 à15
Voies 17 à 31
IT 17 à 31
Signalisation en téléphonie
Trame paire
1 0 0 1 1 0 0 1
IT 1 à 15
Voies 1 à15
Voies 17 à 31
IT 17 à 31
125 µs (longueur 256 bits)

Figure 7.22 Trame MIC et informations de signalisation.

➤ La hiérarchie numérique

La hiérarchie numérique consiste à regrouper des multiplex pour constituer un nouveau multiplex d'ordre supérieur (figure 7.23). Le débit du multiplex de sortie est supérieur à la somme des débits incidents. En effet, le multiplexeur insère dans la trame des informations de services et des bits de justification pour compenser les écarts d'horloge des multiplex incidents (surdébit). Cette hiérarchie est désignée sous le terme de **hiérarchie numérique plésiochrone** (**PDH**, *Plesiochronous Digital Hierarchy*).



Niveau	Pays	Débit en kbit/s	Nombre de voies	Avis de l'UIT-T
Niveau 1	Europe (E1) Japon États-Unis (T1)	2 048 1 544 1 544	30 24 24	G.704
Niveau 2	Europe (E2) Japon États-Unis (T2)	8 448 6 312 6 312	120 96 96	G.742
Niveau 3	Europe (E3) Japon États-Unis (T3)	34 368 33 064 44 736	480 480 672	G.751
Niveau 4	Europe (E4)	139 264	1 920	G.751

Figure 7.23 La hiérarchie numérique PDH.

Constituant la base du réseau numérique de France Télécom depuis 1970, la hiérarchie plésiochrone a été remplacée à partir de 1986 par une nouvelle technique de regroupement appelée **SDH** (*Synchronous Digital Hierarchy*) offrant plus de souplesse dans le démultiplexage et qui autorise des débits supérieurs.

7.3.4 Comparaison multiplexeur/concentrateur

Le multiplexeur a une logique câblée indépendante du protocole, alors que le concentrateur possède une logique programmée donc fortement liée au protocole, comme, par exemple, l'analyse d'adresse du terminal destinataire.

On peut n'utiliser qu'un seul concentrateur par liaison, alors que les multiplexeurs ne s'utilisent que par couple (multiplexage/démultiplexage). Un concentrateur établit une relation de *1 vers n* et de *n vers 1*, un multiplexeur de *1 vers 1*.

La figure 7.24 fournit un exemple d'intégration de multiplexeurs et de concentrateurs dans un réseau d'entreprise.

© Dunod – La photocopie non autorisée est un délit

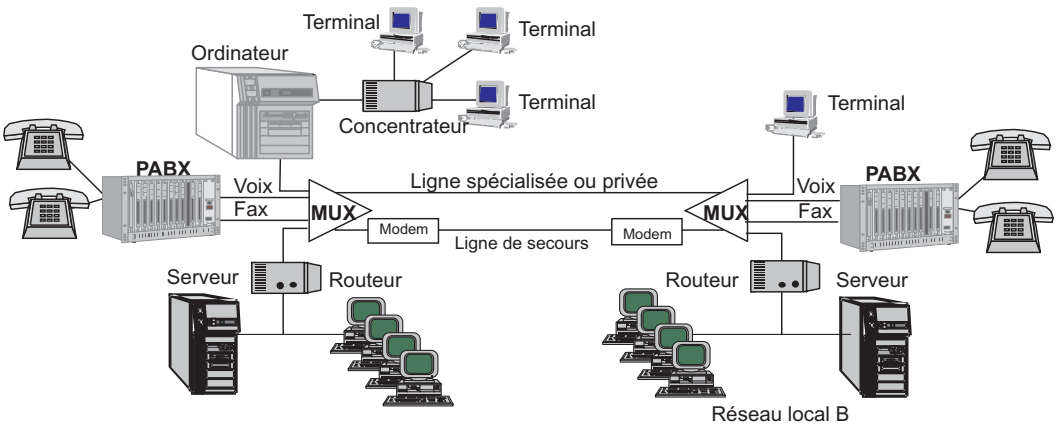


Figure 7.24 Exemple d'utilisation de concentrateurs et de multiplexeurs.

7.4 CONCLUSION

Les multiplexeurs sont un moyen simple de partager un support. Cependant, leur usage est limité, outre que leur connectivité est réduite (relation de 1 à 1), les multiplexeurs ne sont pas adaptés aux mises en relation occasionnelles ni aux transferts sporadiques de données.

Les réseaux apportent une solution à ces problèmes, ils assurent une connectivité ouverte (*1 à 1* parmi *n*, voire *m* parmi *n*) et une mise en relation à la demande. Dans le chapitre suivant nous distinguerons essentiellement 2 types de réseaux : les réseaux en mode circuits, bien adaptés aux flux à débit constant et aux transferts isochrones, et les réseaux en mode paquets qui constituent un véritable système de partage statistique de la bande passante (mutualisation des ressources) et apportent une excellente réponse aux applications à débit variable.

EXERCICES

Exercice 7.1 Intensité de trafic et taux d'activité

Commentez le rapport entre les valeurs de l'intensité de trafic (E) et le taux d'activité (θ), déduisez-en une solution de mutualisation des ressources, donnez un type d'application type.

Exercice 7.2 Application numérique (E et θ)

Caractérisez une liaison de données sachant que :

– le nombre de sessions à l'heure de pointe est de 1 ;
– la durée d'une session est de 10 minutes ;
– l'échange concerne des messages qui au total représentent 120 000 caractères (8 bits) ;
– le débit de la ligne est de 2 400 bit/s.

Déterminez :

a) l'intensité du trafic de la ligne (E) ;

b) le taux d'activité (θ) ;

c) le type d'application possible.

Exercice 7.3 Trame MIC

La trame MIC comporte 32 IT, l'IT0 sert à la synchronisation de la trame, l'IT16 au transport de la signalisation téléphonique (figure 7.25).

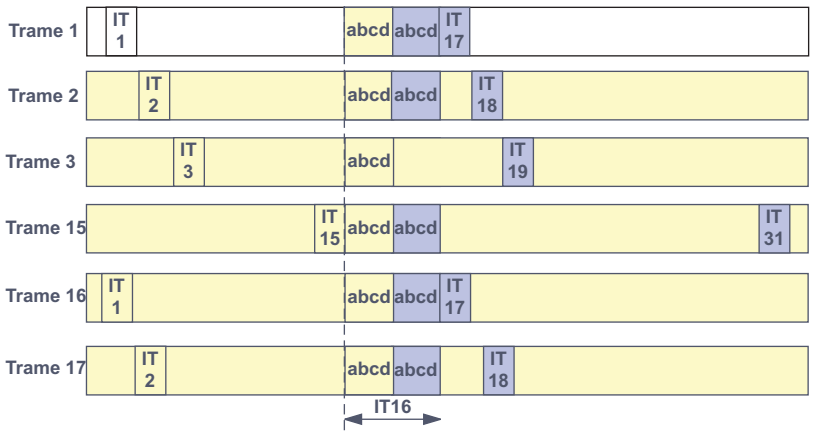


Figure 7.25 Organisation de la trame MIC.

L'IT16 est scindée en 2 quartets (bit a, b, c, d). Le premier quartet de la trame 1 transporte la signalisation téléphonique de la voie 1 (IT1), le second celle de la voie 17 (IT17). De même,

© Dunod – La photocopie non autorisée est un délit

le premier quartet de la trame 2 transporte la signalisation téléphonique de la voie 2 (IT2), le second celle de la voie 18 (IT18)... Cette signalisation est dite par canal associé ou voie par voie (CAS).

a) Quelle est la fréquence de récurrence d'une trame ?

b) Déduisez-en le débit d'une voie, si le signal de voix échantillonnée est supposé être quantifié sur 256 niveaux.

c) Quelle est la fréquence de récurrence du motif de signalisation d'une voie de communication ?

d) Déduisez-en la bande allouée à la signalisation d'une voie ?

Exercice 7.4 Multiplexeur

Un multiplexeur temporel (par intervalle de temps ou IT) supporte « N » voies basse vitesse à 64 000 bit/s chacune (MIC de premier niveau).

a) Sachant que les informations véhiculées résultent d'une numérisation du son sur 256 niveaux de quantification, déterminez la longueur de l'IT, exprimée en bits, sur la liaison composite.

b) Sachant que l'on souhaite transmettre en simultané 30 communications, déterminez le rythme d'occurrence des trames et leur longueur (IT0 est utilisée pour la signalisation de la trame, l'IT16 pour celle des communications).

c) Quel est le débit de la liaison multiplexée correspondante ?

d) Quelle est l'efficacité de multiplexage ?

Chapitre **8**

Le concept de réseau

8.1 GÉNÉRALITÉS

8.1.1 Définitions

Un réseau est un ensemble de moyens matériels et logiciels géographiquement dispersés destinés à offrir un service, comme le réseau téléphonique, ou à assurer le transport de données. Les techniques à mettre en œuvre diffèrent en fonction des finalités du réseau et de la qualité de service désirée.

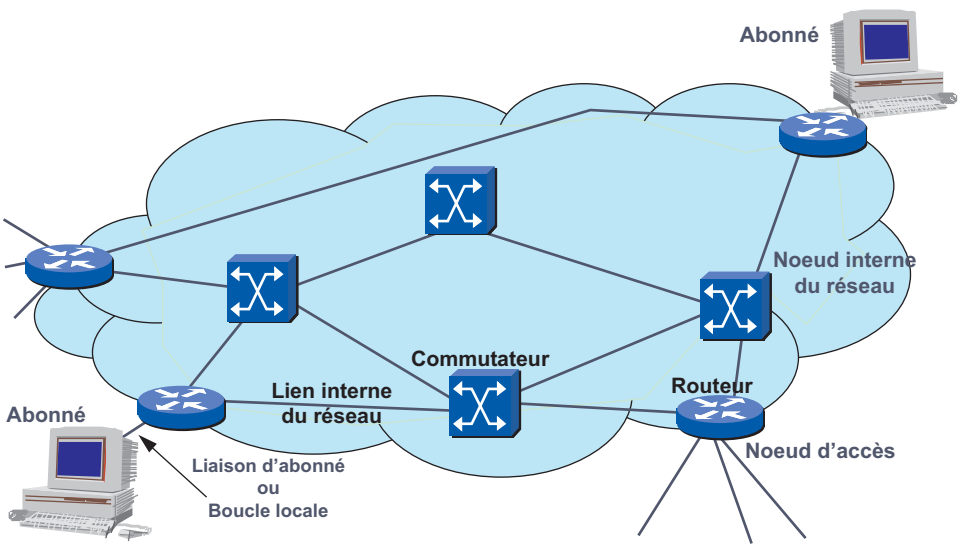


Figure 8.1 Le réseau : ensemble de ressources mises en commun.

Le réseau illustré par la figure 8.1 est composé de nœuds. Les nœuds d'accès, situés à la périphérie du réseau, permettent le raccordement des usagers par une liaison dénommée **liaison d'abonné**. L'ensemble des moyens mis en œuvre pour raccorder un usager est souvent désigné par le terme de **boucle locale**[1]. Les nœuds sont généralement des routeurs au point d'accès et des commutateurs au cœur du réseau.

8.1.2 Classification des réseaux

Le langage courant distingue les réseaux selon différents critères. La classification traditionnelle, fondée sur la notion d'étendue géographique, correspond à un ensemble de contraintes que le concepteur devra prendre en compte lors de la réalisation de son réseau. Généralement, on adopte la terminologie suivante :

- **LAN** (*Local Area Network*), réseau local d'étendue limitée à une circonscription géographique réduite (bâtiment...), ces réseaux destinés au partage local de ressources informatiques (matérielles ou logicielles) offrent des débits élevés de 10 à 100 Mbit/s.
- **MAN** (*Metropolitan Area Network*)**,** d'une étendue de l'ordre d'une centaine de kilomètres, les MAN sont généralement utilisés pour fédérer les réseaux locaux ou assurer la desserte informatique de circonscriptions géographiques importantes (réseau de campus).
- **WAN** (*Wide Area Network*)**,** ces réseaux assurent généralement le transport d'information sur de grande distance. Lorsque ces réseaux appartiennent à des opérateurs, les services sont offerts à des abonnés contre une redevance. Les débits offerts sont très variables de quelques kbit/s à quelques Mbit/s.

D'autres classifications, plus proches des préoccupations quotidiennes, peuvent être adoptées. Le critère organisationnel prédomine. Le réseau est accessible à tous moyennant une redevance d'usage, il est alors dit public ; s'il n'est qu'à une communauté d'utilisateurs appartenant à une même organisation, il est alors dit privé. Un réseau public peut être géré par une personne privée (opérateur de télécommunication de droit privé), et un réseau privé peut être sous la responsabilité d'une personne de droit public (réseau d'un ministère...). Un réseau privé est dit **virtuel** lorsqu'à travers un réseau public on simule (émule) un réseau privé.

Les réseaux se différencient, aussi, selon les modes de diffusion de l'information (figure 8.2). On distingue trois modes :

- La source diffuse ses informations vers des stations réceptrices. La relation est unidirectionnelle de *1 à N* (réseau de diffusion). Les réseaux de radiodiffusion constituent un exemple de ce type de réseau. Les réseaux locaux sont aussi assimilés à cette catégorie.
- À l'inverse, un ensemble de stations peut envoyer les informations à un seul destinataire. La relation est aussi unidirectionnelle, mais de *N à 1* (réseaux de collecte). Les réseaux de télémesure constituent un exemple de ce mode de fonctionnement.
- D'une manière plus générale, un abonné d'un réseau désire pouvoir atteindre tous les autres abonnés ou une partie de ceux-ci. Le réseau doit établir une relation de *1 à 1* parmi *N*. Ces réseaux, de mise en relation, sont dits **réseaux de commutation**, le réseau téléphonique (RTC) en est un exemple.

1. Pour certains la boucle locale ne comprend que la liaison cuivre qui relie l'abonné au PoP (*Point of Presence*).

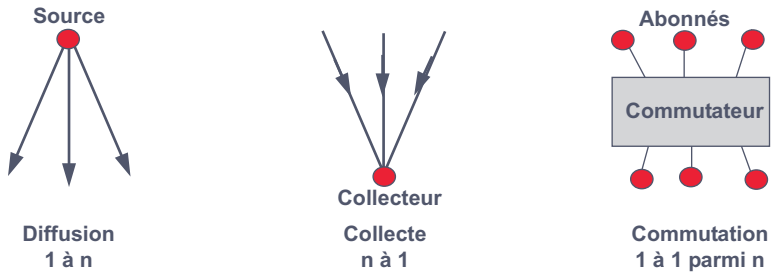


Figure 8.2 Classification selon les modes de diffusion de l'information.

Enfin, une autre distinction (approche temporelle) applicable à tous les réseaux décrit comment les différents nœuds (éléments actifs) d'un réseau sont synchronisés entre eux (figure 8.3) :

– Si chaque nœud a une horloge indépendante**,** le réseau est dit **plésiochrone** . Les horloges réception et émission sont différentes mais proches (plésio).

– Si les horloges des différents nœuds sont toutes asservies à une même horloge, le réseau est dit **synchrone**. L'horloge principale peut être une horloge atomique ou une horloge pilotée par les tops horaires d'un GPS.

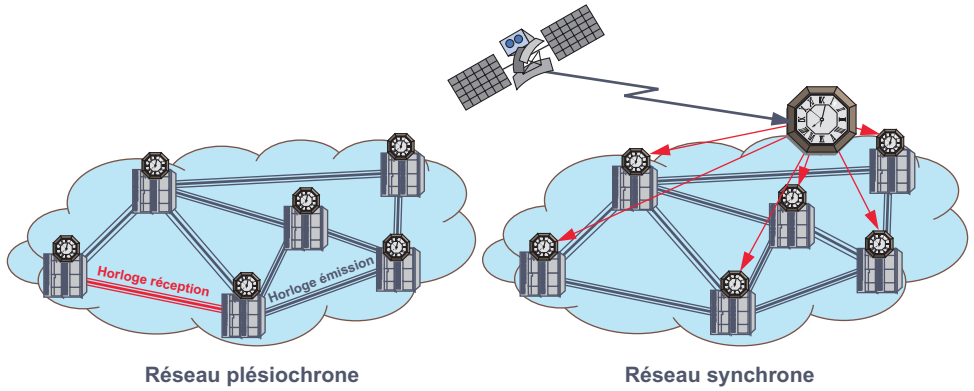


Figure 8.3 Distinction des types de réseaux selon le mode de synchronisation.

La synchronisation des réseaux et les problèmes en relation avec la distribution des horloges constituent un problème majeur de conception d'un réseau. L'étude de ces techniques sort du cadre de cet ouvrage.

8.1.3 Topologies physiques des réseaux

La topologie d'un réseau décrit la manière dont les nœuds sont connectés. Cependant, on distingue la **topologie physique**, qui décrit comment les machines sont raccordées au réseau, de la **topologie logique** qui renseigne sur le mode d'échange des messages dans le réseau (**topologie d'échange**).

© Dunod – La photocopie non autorisée est un délit

Les topologies de base

Les topologies de bases sont toutes des variantes d'une liaison point à point ou multipoint (figure 8.4).

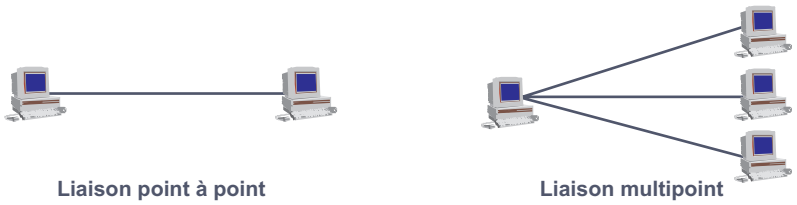


Figure 8.4 Les modes de liaisons élémentaires.

La plus simple des topologies de base, le **bus** est une variante de la liaison multipoint. Dans ce mode de liaison, l'information émise par une station est diffusée sur tout le réseau. Le réseau en bus est aussi dit **réseau à diffusion** (figure 8.5). Dans ce type de topologie, chaque station accède directement au réseau, d'où des problèmes de conflit d'accès (contentions ou collisions) qui nécessitent de définir une politique d'accès. Celle-ci peut être centralisée (relation dite maître/esclave) ou distribuée comme dans les réseaux locaux.

Les réseaux en bus sont d'un bon rapport performance/prix. Ils autorisent des débits importants (>100 Mbit/s sur 100 m). Il est possible d'y insérer une nouvelle station sans perturber les communications en cours. Cependant, la longueur du bus est limitée par l'affaiblissement du signal, il est nécessaire de régénérer celui-ci régulièrement. La distance entre deux régénérations se nomme « pas de régénération ».

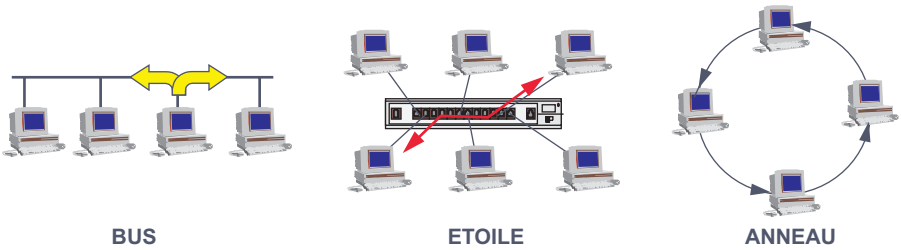


Figure 8.5 Les topologies de base.

La topologie étoile est une variante de la topologie en point à point. Un nœud central émule *n* liaisons point à point (figure 8.5). Tous les nœuds du réseau sont reliés à un nœud central commun : le concentrateur. Tous les messages transitent par ce point central. Le concentrateur est actif, il examine chaque message reçu et ne le retransmet qu'à son destinataire. Cette topologie correspond, par exemple, au réseau téléphonique privé d'une entreprise où le commutateur téléphonique met en relation les différents postes téléphoniques de l'installation. La topologie étoile autorise des dialogues internoeud très performants. La défaillance d'un poste n'entraîne pas celle du réseau, cependant le réseau est très vulnérable à celle du nœud central.

Dans la topologie en anneau, chaque poste est connecté au suivant en point à point (figure 8.5). L'information circule dans un seul sens, chaque station reçoit le message et le régénère. Si le message lui est destiné, la station le recopie au passage (au vol). Ce type de connexion autorise des débits élevés et convient aux grandes distances (régénération du signal

par chaque station). L'anneau est sensible à la rupture de la boucle. Les conséquences d'une rupture de l'anneau peuvent être prises en compte en réalisant un double anneau[2].

Les topologies construites

Dérivés des réseaux en étoile, les réseaux arborescents (figure 8.6 gauche) sont constitués d'un ensemble de réseaux étoiles reliés entre eux par des concentrateurs jusqu'à un nœud unique (nœud de tête). Cette topologie est essentiellement mise en œuvre dans les réseaux locaux (Starlan, 10 base T...). Ces réseaux, en raison de la concentration réalisée à chaque nœud, sont très vulnérables à la défaillance d'un lieu ou d'un nœud (figure 8.6 centre).

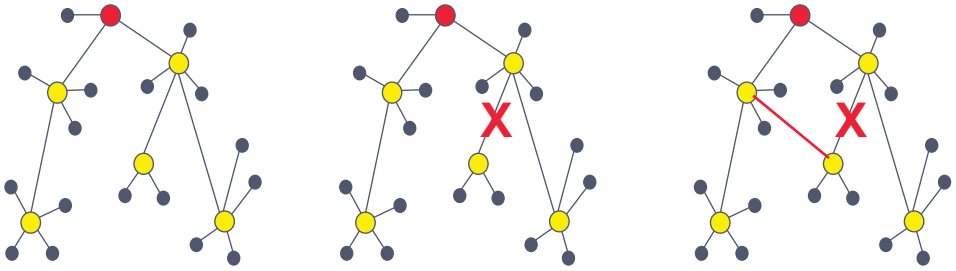


Figure 8.6 De la topologie hiérarchique à la topologie maillée.

Pour palier cet inconvénient on peut imaginer créer des chemins de secours qui peuvent être temporaires ou permanents. Le réseau est alors dit **maillé** (figure 8.6 droite). Un réseau maillé est un réseau dans lequel deux stations, clientes du réseau, peuvent être mises en relation par différents chemins (figure 8.7). Ce type de réseau, permettant de multiple choix de chemins vers une même destination, est très résistant à la défaillance d'un nœud et autorise une optimisation de l'emploi des ressources en répartissant la charge entre les différents nœuds (voies). Chaque nœud est caractérisé par sa **connectivité**, c'est-à-dire par le nombre de liens qui le réunit aux autres nœuds du réseau.

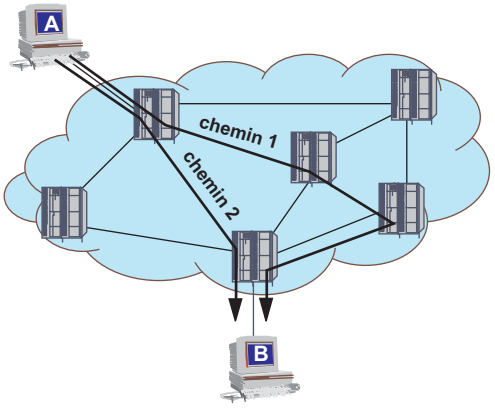


Figure 8.7 Réseau maillé.

2. La technique du double anneau est mise en œuvre dans les réseaux métropolitains comme le FDDI (voir section 13.2).

© Dunod – La photocopie non autorisée est un délit

8.2 LES RÉSEAUX À COMMUTATION

8.2.1 Introduction à la commutation

Le concept de réseau à commutation est né de la nécessité de mettre en relation un utilisateur avec n'importe quel autre utilisateur (relation de *1 à* 1 parmi *n* ou interconnexion totale) et de l'impossibilité de créer autant de liaisons point à point qu'il y a de paires potentielles de communicants.

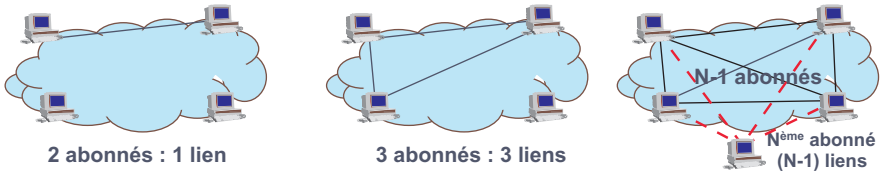


Figure 8.8 L'interconnexion totale.

Ainsi, pour réaliser l'interconnexion totale de 2 stations (figure 8.8), il suffit d'une liaison, pour 3 stations 3 liens... D'une manière générale, dans un réseau de N stations, pour relier la station N aux $N-1$ stations déjà connectées il faut $(N-1)$ liens. Soit, pour les N stations, $N(N-1)$ liens. En comptant de cette manière, on commet l'erreur de compter deux fois chaque lien (le lien de A vers B est le même que le lien de B vers A). Le nombre total de liens nécessaires dans un système de N nœuds est donc de :

$$\text{Nombre de liens} = \frac{N(N-1)}{2}$$

Si on applique cette formule au réseau téléphonique, compte tenu qu'il existe environ 300.10^6 abonnés dans le monde et que chaque abonné peut être mis en relation avec n'importe quel autre abonné, la terminaison de réseau chez chaque abonné devrait comporter 45.10^{15} lignes !

Ce chiffre montre, s'il en était besoin, la nécessité de trouver un système qui permette, à partir d'une simple ligne de raccordement (liaison d'abonné), d'atteindre simplement tout autre abonné du réseau par simple commutation d'un circuit vers cet abonné. Ce système porte le nom de **réseau à commutation**, dans le réseau illustré par la figure 8.9, le commutateur met en relation les utilisateurs A et B.

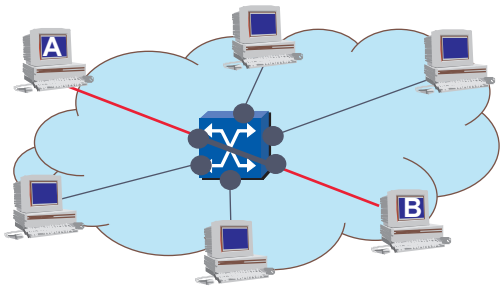


Figure 8.9 Principe d'un réseau à commutation.

Dans ce contexte où la ressource est rare vis-à-vis de la demande potentielle (si simultanément tous les abonnés du réseau désiraient joindre un autre abonné...), il est indispensable de rechercher des techniques particulières pour optimiser le partage des ressources, c'est l'objectif des techniques de commutation. Selon la technique employée pour « relier » deux utilisateurs, on distingue la commutation de circuits, de messages ou de paquets.

Un réseau à commutation assure une connectivité totale. Dans ses conditions, la topologie logique ou interconnexion totale, vue du côté des utilisateurs, est différente de la topologie physique réelle (figure 8.10).

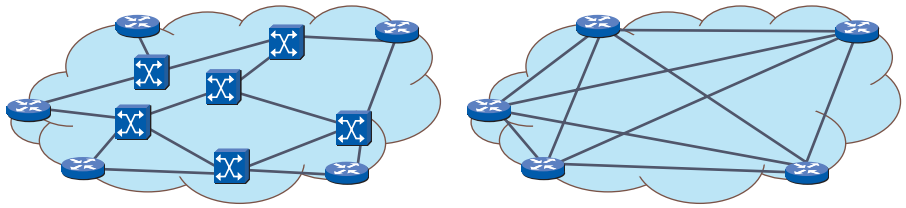


Figure 8.10 Conséquence de la commutation sur la vision du réseau.

8.2.2 La commutation de circuits

Dans la commutation de circuits, un lien physique est établi par juxtaposition de différents supports physiques afin de constituer une liaison de bout en bout entre une source et une destination (figure 8.11). La mise en relation physique est réalisée par les commutateurs avant tout échange de données et est maintenue tant que les entités communicantes ne la libèrent pas expressément. Le taux de connexion est important, alors que le taux d'activité peut être faible.

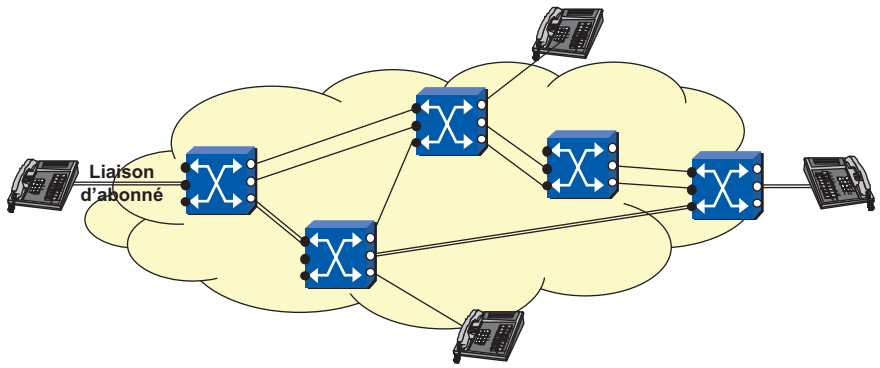


Figure 8.11 Réseau à commutation de circuits ou spatiale.

La constitution d'un chemin physique, emprunté par la suite par toutes les données transférées, garantit l'ordonnancement des informations. Elles sont reçues dans l'ordre où elles ont été émises. Cependant, les deux entités correspondantes doivent être présentes durant tout l'échange de données, il n'y a pas de stockage intermédiaire. Les débits de la source et du destinataire doivent être identiques. Les abonnés monopolisent toute la ressource durant la connexion. Dans ces conditions, la facturation est généralement dépendante du temps et de la distance (exemple : le Réseau Téléphonique Commuté ou **RTC**).

© Dunod – La photocopie non autorisée est un délit

Archétype des réseaux, la commutation de circuits ou commutation spatiale est aujourd'hui remplacée par une commutation par intervalle de temps (IT) entre des multiplex entrants et des multiplex sortants (commutation temporelle, figure 8.12).

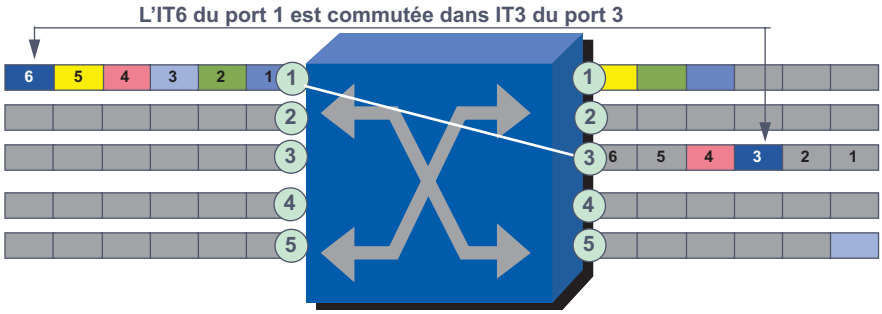


Figure 8.12 La commutation temporelle.

8.2.3 La commutation de messages

En commutation de circuits, la régulation de trafic est réalisée à la connexion, s'il n'y a plus de ressource disponible, de bout en bout, la connexion est refusée. Pour éviter d'avoir à sur-dimensionner les réseaux, la commutation de messages, n'établit aucun lien physique entre les deux systèmes d'extrémité. Le message est transféré de nœud en nœud et mis en attente si le lien internœud est occupé (figure 8.13). Chaque bloc d'information (message) constitue une unité de transfert (fichier, écran de terminal...) acheminée individuellement par le réseau. Le message est mémorisé, intégralement, par chaque nœud, et retransmis au nœud suivant dès qu'un lien se libère. Le transfert réalisé, le lien est libéré. Assurant une meilleure utilisation des lignes, la commutation de messages autorise un dimensionnement des réseaux à commutation de messages inférieur à celui des réseaux à commutation de circuits. En cas de fort trafic, il n'y a pas blocage du réseau mais seulement un ralentissement (attente de la libération d'un lien). La mémorisation intermédiaire de l'intégralité des messages nécessite des mémoires de masse importantes et augmente le temps de transfert. Les réseaux à commutation de messages ne sont pas adaptés aux applications interactives.

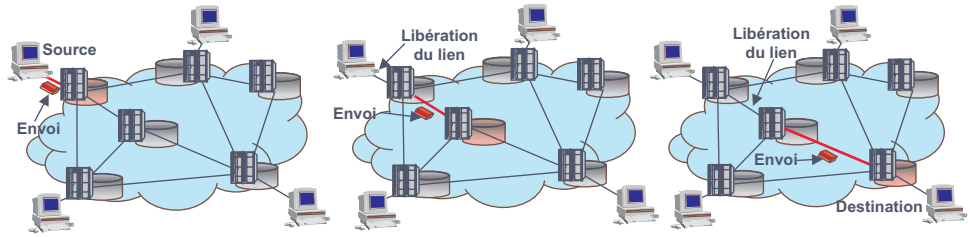


Figure 8.13 Principe de la commutation de messages.

Les réseaux à commutation de messages assurent, par rapport à la commutation de circuits :

– le transfert, même si le correspondant distant est occupé ou non connecté ;
– la diffusion d'un même message à plusieurs correspondants ;
– le changement de format des messages ;
– l'adaptation des débits et éventuellement des protocoles.

La commutation de messages ne permet qu'un échange **simplex et asynchrone**, elle est plus un service qu'une technique réseau. La commutation de messages est aujourd'hui le support logique des réseaux de télex et des systèmes de messagerie modernes.

8.2.4 La commutation de paquets

Principe

La commutation de paquets utilise une technique similaire à la commutation de messages. Le message est découpé en fragments (paquets) de petite taille. Chaque paquet est acheminé dans le réseau indépendamment du précédent. Contrairement à la commutation de messages, il n'y a pas de stockage d'information dans les nœuds intermédiaires. Chaque nœud, recevant un paquet, le réémet immédiatement sur la voie optimale. De ce fait, le séquencement des informations n'est plus garanti. Pour reconstituer le message initial, le destinataire devra, éventuellement, réordonnancer les différents paquets avant d'effectuer le réassemblage.

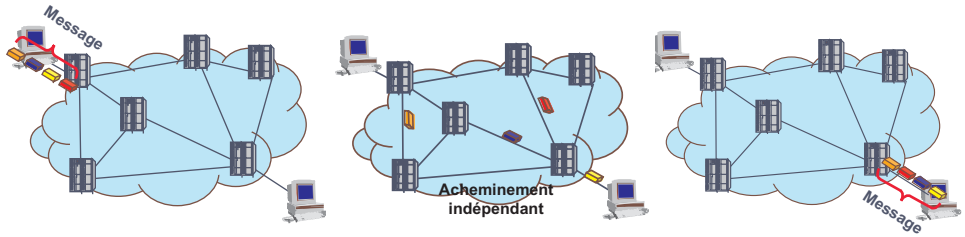


Figure 8.14 Principe de la commutation de paquets.

Ce mode de transfert optimise l'utilisation des ressources, les paquets de différentes sources sont multiplexés sur un même circuit. Cependant, chaque paquet doit contenir les informations nécessaires à son acheminement ou un label identifiant le flux (multiplexage par étiquette). La ressource offerte est banalisée et non attribuée à une communication particulière comme dans la commutation de circuits (figure 8.15).

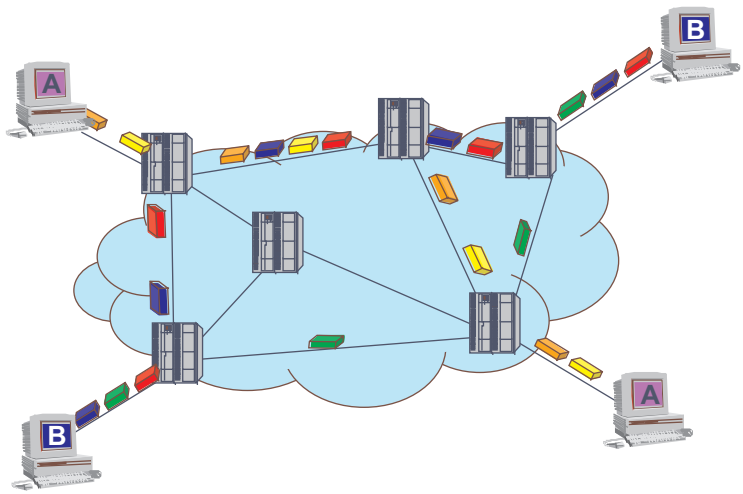


Figure 8.15 Le multiplexage des sources dans le réseau.

La commutation de paquets et le multiplexage par étiquette sont des techniques similaires.

© Dunod – La photocopie non autorisée est un délit

Elles se différencient essentiellement par le fait que l'une admet des unités de données de taille variable (commutation de paquets), l'autre des unités de données de taille fixe (multiplexage par étiquette). Le multiplexage par étiquette est aussi nommé **commutation de cellules**. Cette dernière technique est utilisée par le protocole **ATM** (voir chapitre 11).

Performance

Supposons que dans le réseau illustré par la figure 8.16, tous les paquets d'un même message empruntent la même route. En admettant que le temps de transfert sur le support et que le temps de traitement soient nuls, seul le temps d'émission des paquets sur le support intervient pour déterminer les performances.

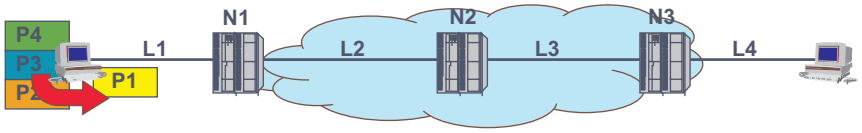


Figure 8.16 Performance d'un réseau à commutation de paquets.

Le message de longueur L (en bits) est découpé en p paquets émis sur les différents supports à un même débit de D bit/s. À l'instant t_0, le paquet 1 est émis sur le lien 1. Ce paquet est reçu par le nœud 1 à $t_0 + t_p$ où t_p est le temps de transmission d'un paquet. En admettant que le temps de traitement dans le nœud soit nul, le paquet est réémis immédiatement sur le nœud 2, pendant que le paquet 2 est émis sur le lien 1...

Si N est le nombre de nœuds, le paquet 1 arrive à destination à :

$$(N + 1)t_p$$

Si p est le nombre de paquets, le dernier paquet est émis à :

$$(p - 1)t_p$$

Le dernier paquet arrive à (ce qui correspond à la fin du transfert) :

$$(p - 1)t_p + (N + 1)t_p$$

Soit encore,

$$t_p(p + N)$$

En posant $t_p = L/pD$, on obtient le temps de traversée du réseau (Tp) :

$$Tp = (L/pD)(p + N)$$

Ou encore

$$Tp = L/D(1 + N/p)$$

Cependant, cette formule ne prend pas en compte les données protocolaires (H) qu'il convient d'ajouter à chaque paquet, d'où :

$$Tp = (\frac{L + pH}{D})(1 + \frac{N}{p})$$

La courbe de la figure 8.17 traduit graphiquement ce résultat. Les valeurs sont exprimées par rapport à la commutation de messages (p = 1 et N > 0), en formulant les hypothèses suivantes : L = 1 500 octets, N = 5.

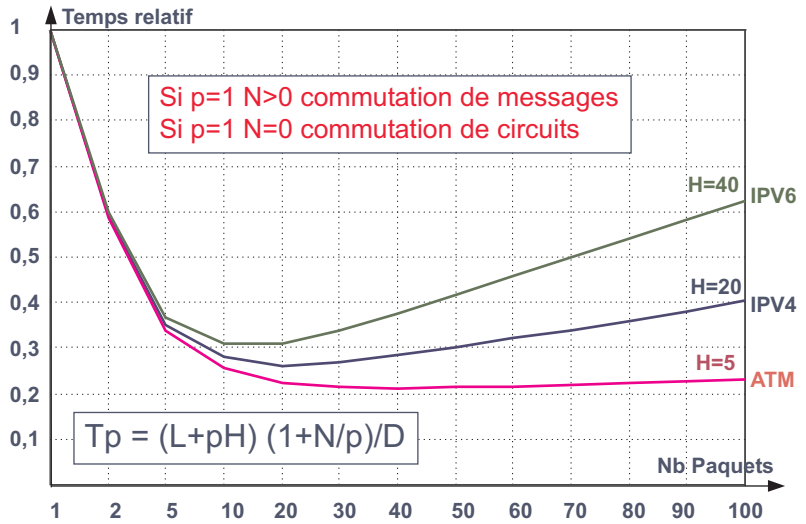


Figure 8.17 Évolution du temps de transit en fonction du nombre de paquets.

Discussion :

- Le temps de transit dans le réseau est d'autant plus faible que le facteur N est petit. Ce qui conduit à rechercher des routes qui minimisent le nombre de nœuds traversés (algorithmes de routage) et à augmenter le maillage du réseau (augmentation de la probabilité de trouver une route plus directe).
- L'influence de la taille de l'en-tête de service est non négligeable, la figure compare les performances en fonction d'un en-tête ATM (5 octets), IPV4 (20 octets) et IPV6 (40 octets). Cette approche conduit à définir un rapport optimal entre la charge utile du bloc de données et les données de services.
- Notons qu'en cas d'erreur, en commutation de messages, le message est intégralement retransmis, en commutation de paquets seul le paquet erroné ou, si on utilise un mécanisme d'anticipation tous les paquets depuis le paquet erroné dans la fenêtre sont retransmis.

Commutation de circuits ou de paquets ?

Rappelons qu'en commutation de paquets, à chaque paquet, le nœud recherche une route optimale. Dans ces conditions, le séquencement des paquets n'est pas garanti. La reprise sur erreur et le contrôle de flux nécessitant une stabilité de route ne sont, par conséquent, pas réalisables.

© Dunod – La photocopie non autorisée est un délit

Le réseau est dit *best effort* (pour le mieux), l'unité de données porte alors le nom de **datagramme**.

Entre le mode datagramme qui optimise l'utilisation des ressources mais ne garantit pas l'acheminement des données et la commutation de circuits, pourrait-on imaginer (figure 8.18) une solution qui garantisse le séquencement des données, permette la reprise sur erreur et autorise un contrôle de flux (commutation de circuits) tout en optimisant l'utilisation du réseau (commutation de paquets) ?

	Commutation de circuits	Commutation de paquets
Établissement d'un circuit	Préalable à l'échange de données	Pas de circuit préétabli
Garantie du séquencement	**OUI**	Non
Optimisation des ressources	Non, Circuit dédié	**OUI, Circuit partagé**
Indépendance des débits	Non	**OUI**

Figure 8.18 Comparaison entre la commutation de paquets et de circuits

Le cumul des avantages de l'un et de l'autre conduit à émuler un circuit dans les réseaux à commutation de paquets. Ainsi, la commutation de paquets décline deux modes de mise en relation (figure 8.19). Le premier, le mode datagramme ou non connecté est le mode naturel de la commutation de paquets. Le second met en œuvre un mécanisme de stabilité de route qui consiste à « baliser » un chemin que suivront ensuite tous les paquets émulant ainsi un circuit sur un réseau en mode paquets. Ce second mode de fonctionnement est dit mode orienté connexion ou plus simplement mode connecté. Le circuit émulé porte le nom de circuit virtuel (**CV**).

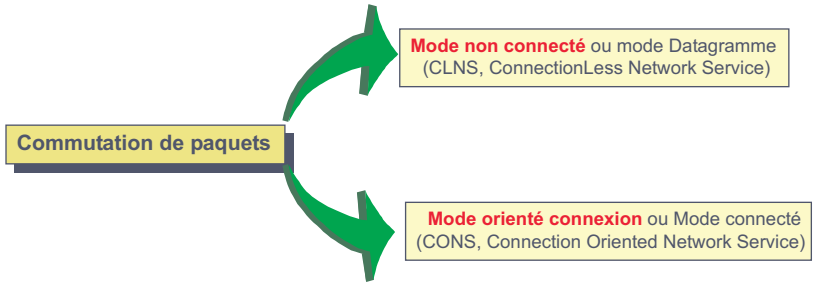

Commutation de paquets
Mode non connecté ou mode Datagramme
(CLNS, ConnectionLess Network Service)
Mode orienté connexion ou Mode connecté
(CONS, Connection Oriented Network Service)

Figure 8.19 Les modes de mise en relation

Les modes de mise en relation

➤ Le mode non connecté (CLNS)

En **mode non connecté** (**CLNS**, *ConnectionLess Network Service*), les informations transitent dans le réseau indépendamment les unes des autres. Le destinataire n'est pas nécessairement à l'écoute, les informations sont, dans ce cas, perdues. Dans un tel mode de fonctionnement, les routes empruntées par les différents blocs d'information peuvent être différentes, le séquencement des informations ne peut être garanti (figure 8.20).

Les mécanismes réseaux sont allégés au détriment d'une complexité dans les organes d'extrémités qui doivent être capables de réordonnancer les différents blocs d'information.

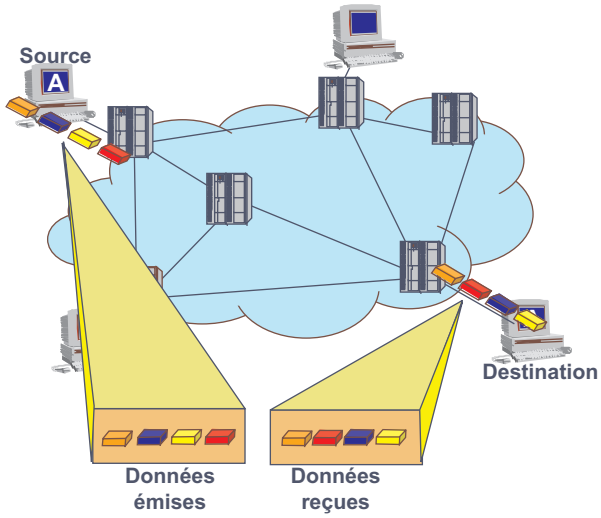


Figure 8.20 Réseau en mode datagrammes

La possibilité d'un routage différent pour chaque bloc d'information (paquet) d'un même utilisateur permet de répartir la charge du réseau (routage adaptatif). Chaque bloc est acheminé indépendamment du précédent, il doit, par conséquent, contenir l'adresse du destinataire. Aucune réservation de ressources n'est effectuée préalablement à tout envoi de données. De ce fait, en cas de surcharge du réseau, des blocs d'information peuvent être perdus.

➤ Le mode orienté connexion (CONS)

En commutation de circuits une liaison physique est préalablement établie avant tout échange de données. En **mode orienté connexion** (**CONS**, *Connection Oriented Network Service*), une liaison virtuelle est construite par un mécanisme particulier (figure 8.21). Lors de la phase d'établissement de la connexion, les différentes ressources nécessaires au transfert (buffers, voies...) sont réservées. Lorsque l'échange est terminé, une phase de déconnexion libère les ressources. La liaison peut être permanente (**CVP**, Circuit Virtuel Permanent ou **PVC,** *Permanent Virtual Circuit*) ou établie appel par appel (**CVC**, Circuit Virtuel Commuté ou **SVC,** *Switched Virtual Circuit*).

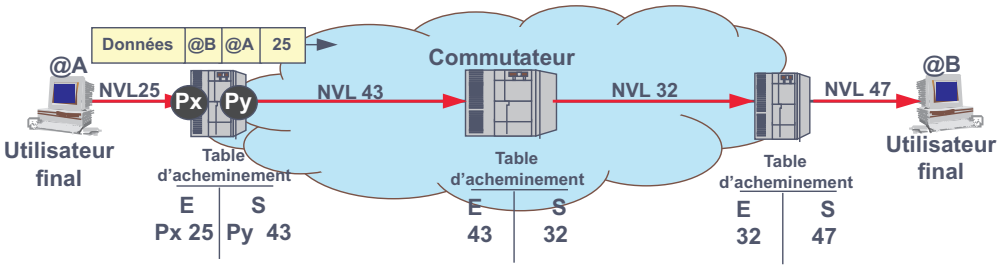


Figure 8.21 Établissement d'un circuit virtuel.

À l'établissement du circuit virtuel, un message spécifique (paquet d'établissement) est routé dans le réseau. Son acheminement est enregistré dans les commutateurs et identifié par un numéro appelé Numéro de Voie Logique (**NVL**). Dans l'exemple, illustré par la figure 8.21,

© Dunod – La photocopie non autorisée est un délit

la source émet le paquet d'établissement. Celui-ci contient les informations utiles à son acheminement dans le réseau (adresses source et destination) et un label attribué par la source pour identifier par la suite le flux de données. Dans cet exemple le label ou Numéro de Voie Logique attribué est 25. Le nœud d'accès au réseau mémorise qu'il a reçu par son port *Px* un flux identifié par le NVL 25, en fonction de l'adresse destination et de l'état du réseau, il achemine le paquet sur son port *Py*. Compte tenu qu'il avait déjà précédemment identifié sur cette voie 42 autres communications, il substitue le label 43 (43^{e} flux) au label 25 de la source. Il mémorise ses informations dans sa table d'acheminement. Par la suite, tout paquet entrant par le port *Px* et identifié par le NVL 25 sera acheminé sur le port *Py* avec le label 43. Chaque nœud jusqu'à destination procède de même. Le circuit virtuel est établi, il résulte de la concaténation des voies logiques 25, 43, 32 et 47.

Durant la phase d'établissement du circuit, les différentes ressources nécessaires au transfert de données sont réservées (buffers, voies...). Ensuite, tous les messages empruntent la route préétablie, le séquencement des informations est garanti (chemin identique). À la fin de l'échange, une phase de déconnexion libère les ressources.

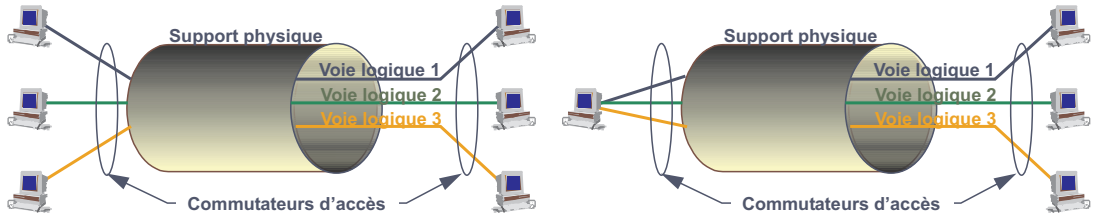


Figure 8.22 Multpiplexage de voies logiques sur une voie physique.

Le système du circuit virtuel (figure 8.22) autorise d'une part, le partage d'un même lien physique par plusieurs entités communicantes indépendantes et, d'autre part, la communication d'un même système avec plusieurs autres systèmes, chaque liaison étant identifiée localement par son numéro de voie logique.

➤ Réseau en mode connecté ou en mode datagramme ?

Un service en mode connecté ou non connecté ne dépend pas du service support utilisé, mais des protocoles mis en œuvre sur ce support. Définir, pour un réseau, le type de protocole à utiliser, résulte d'un choix essentiellement fondé sur les performances et la qualité de service que l'on désire obtenir. Le tableau de la figure 8.23 compare les deux modes de mise en relation.

➤ Circuit virtuel commuté ou permanent ?

Un circuit virtuel commuté est une liaison établie à la demande, il autorise l'établissement d'une relation avec n'importe quel autre abonné du réseau, la connectivité est ouverte. Le circuit virtuel permanent est établi (configuré) une fois pour toutes, la connectivité est réduite.

En principe, tous les protocoles réseaux en mode connecté offrent les deux possibilités. Cependant, dans les réseaux haut débit, compte tenu de la puissance de calcul nécessaire à l'établissement d'un circuit virtuel commuté, les opérateurs n'offrent, actuellement, que le service en CVP (Circuit Virtuel Permanent ou SVP). La définition d'un raccordement à un tel réseau est toujours précédée d'une analyse des besoins de connectivité de l'entreprise. Cette connectivité est décrite dans une matrice de communication. La matrice de communication

Critères	Mode orienté connexion	Mode non connecté
Mise en relation nécessaire	Obligatoire.	Non.
Délai de connexion **Délai de déconnexion**	Oui, pouvant être important.	Non, puisque pas de connexion.
Type de circuit offert	Permanent durant tout l'échange.	Pas de circuit réservé, mode datagramme.
Allocation de ressources	Oui, statique (à la connexion).	Non.
Contrôle de flux possible	Oui.	Non.
Séquencement des informations	Oui (garanti par le réseau).	Non (à charge du destinataire).
Reprise sur incident	Oui.	Non.
Complexité	Couche réseau	Couche transport
Optimisation des réseaux	Non, circuits et ressources réservés durant toute la relation.	Oui, pas de ressource réservée, optimisation lors du routage.
Résistance à la défaillance	Non, en cas de défaillance, il faut reconstituer un circuit virtuel.	Oui, pas de chemin préétabli, en cas de défaillance d'un lien ou d'un nœud reroutage sur une autre voie.
Adressage	Simplifié, label attribué à la connexion.	Complet, chaque bloc de données (paquet) contient l'adresse complète source et destination.

Figure 8.23 Comparaison entre le mode non connecté et orienté connexion.

indique, pour chaque liaison, le flux de données estimé afin de définir les caractéristiques de chaque abonnement. Dans l'exemple de la figure 8.24, seul le besoin de communication a été indiqué. Dans le réseau résultant, si A veut communiquer avec E, ses messages devront transiter par C et D, cette solution est souvent adoptée quand les flux de ce type (A vers E) sont faibles.

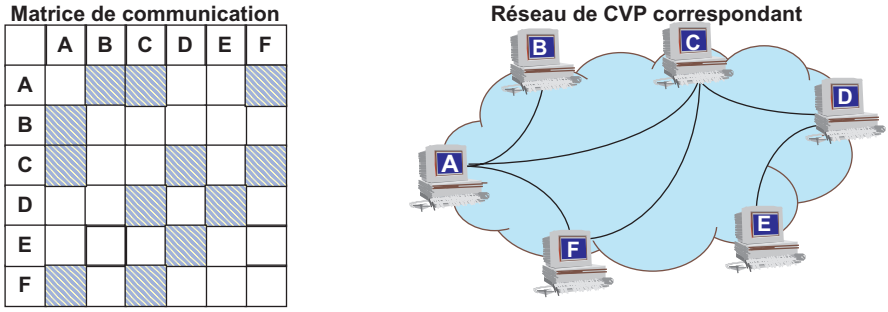


Figure 8.24 Matrice de communication et réseau logique correspondant.

8.2.5 Les mécanismes mis en œuvre dans le réseau

L'échange, à travers un ou plusieurs réseaux, entre deux entités communicantes quelconques, nécessite que :

– chaque correspondant puisse être localisé et identifié de manière unique sur le réseau, c'est la notion **d'adressage** et de **nommage** ;

– en fonction des éléments ci-dessus, le réseau assure l'acheminement des blocs d'information, c'est le **routage** ;

© Dunod – La photocopie non autorisée est un délit

– la taille des unités de données transférées soit adaptée aux capacités du réseau, c'est la **segmentation** ;
– des mécanismes de contrôle sont mis en œuvre pour garantir que le trafic admis dans le réseau ne conduira pas à l'effondrement de celui-ci, c'est le **contrôle de congestion** ;

8.3 NOTION D'ADRESSAGE

8.3.1 Définitions

On désigne par technique d'adressage l'ensemble des moyens utilisés pour identifier les correspondants. Pour assurer la communication, le système d'extrémité source doit fournir au réseau l'adresse du système d'extrémité destinataire (adresse destinataire), et celui-ci doit pouvoir identifier son correspondant (adresse source).

Une adresse est une suite de caractères désignant sans ambiguïté un point physique de raccordement à un réseau (adressage physique) ou identifiant un processus, une machine (adressage logique). Ces deux notions sont complémentaires, l'une désigne l'objet (adresse logique), l'autre sa localisation (adresse physique).

8.3.2 L'adressage physique

Généralités

L'adresse des correspondants raccordés à un réseau est un identifiant qui permet l'acheminement à travers un ou plusieurs réseaux d'un message vers son destinataire. Pour localiser un utilisateur final sans ambiguïté, il faut pouvoir identifier (figure 8.25) :

– le réseau auquel il est connecté ;
– le point d'accès auquel il est raccordé au réseau, ce point identifie aussi l'installation locale de l'abonné ;
– le système cible dans l'installation locale.

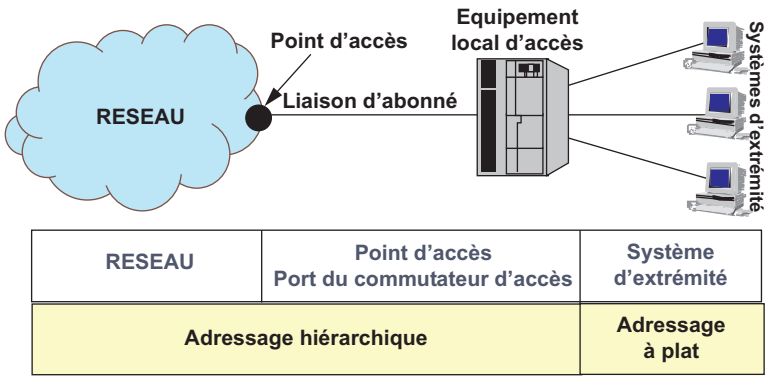


Figure 8.25 Les composantes d'une adresse.

Les deux premiers champs permettent de localiser l'installation de l'abonné, il constitue l'adresse réseau du destinataire, la structure est généralement du type hiérarchique. Le troi-

sième champ identifie le destinataire dans l'installation finale, il peut alors être sans signification, il est alors dit **à plat**.

L'adressage à plat ou global

Dans ce type d'adressage, l'adresse correspond à un numéro unique attribué sans aucune règle de structuration. Cet adressage est, par exemple, celui utilisé dans les réseaux locaux. Chaque entité raccordée a un numéro différent et sans relation avec n'importe quel autre numéro (adresse) du réseau. D'origine Xerox, cet adressage destiné à distinguer les différents nœuds d'un même segment de réseau est normalisé par l'IEEE[3] (figure 8.26). Identifiant, dans les réseaux locaux, le point d'accès au support, cet adressage est souvent appelé adressage **MAC** (*Medium Access Control*).

<table>
<tr><td colspan="4">48 bits.</td></tr>
<tr><td>I/G</td><td>U/L</td><td>Identification par l'IEEE du constructeur.</td><td>Numéro séquentiel attribué par le constructeur</td></tr>
<tr><td colspan="2"></td><td>22 bits.
2^{22} constructeurs</td><td>24 bits.
2^{24} hosts-2.</td></tr>
</table>

Figure 8.26 L'adressage MAC ou IEEE (réseaux locaux).

L'adressage MAC comporte deux champs. Le premier, champ attribué par l'IEEE, désigne le constructeur (**OUI**, *Organizationaly Unit Identifier*) de l'interface réseau (**NIC**, *Network Interface Card*). La liste des OUI attribués peut être obtenue dans la RFC 1340. Le second champ correspond à un numéro séquentiel attribué par le constructeur qui doit en garantir l'unicité.

L'adresse MAC peut identifier un point de raccordement unique (cas général), elle est alors dite *unicast*. Elle peut aussi désigner un groupe de machines raccordées à un segment du réseau elle est, alors, dite de *multicast*. L'adresse MAC peut aussi représenter toutes les machines d'un réseau du même réseau physique, dans ce dernier cas on parle d'adresse de diffusion généralisée ou *broadcast*.

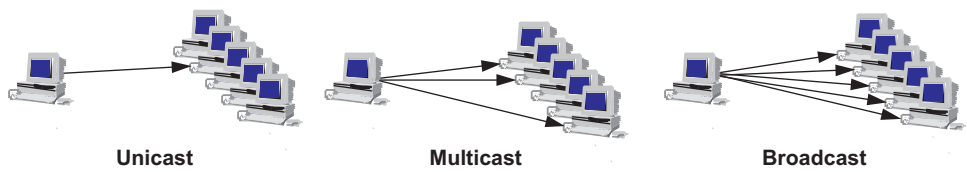


Figure 8.27 Adressage et points adressés.

L'adressage hiérarchique

Utilisée dans les grands réseaux d'interconnexion, l'adresse hiérarchique identifie un point d'accès au réseau. Son contenu est significatif, il désigne le réseau et les nœuds de ce réseau participant à l'acheminement des informations. Chaque nœud ne traite que la partie d'adresse

3. Notons que l'IEEE a récemment introduit la notion d'identifiant d'interface sur 64 bits (36 + 24), cet identifiant d'interface est désigné sous le terme EUI-64 (*End-User Identifier*).

© Dunod – La photocopie non autorisée est un délit

correspondant à son niveau. Cette technique permet de réduire le champ adresse des blocs de données au fur et à mesure de la progression des blocs dans le réseau.

L'adressage définit par l'ISO dit adressage **NSAP**[4] (*Network Service Access Point*) représenté figure 8.28 définit plusieurs champs :

– **L'AFI** (*Autority Format Identifier*), désigne l'autorité gestionnaire du domaine d'adressage et le format de représentation de l'adresse. La valeur 37 indique que l'adresse qui suit est au format X.121 et est codée en DCB[5].

– **L'IDI** (*Initial Domain Identification*), identifie le domaine d'adressage. Dans la norme X.121 (AFI = 37), le numéro 208 est affecté à la France, le 2 représentant l'Europe.

– **DSP** (*Domain Specific Part*), correspond à l'adresse effective de l'abonné.

– Cette adresse peut éventuellement être complétée par l'adresse du terminal dans l'installation d'abonné, ici nous avons joint à cette adresse l'adresse IEEE du terminal.

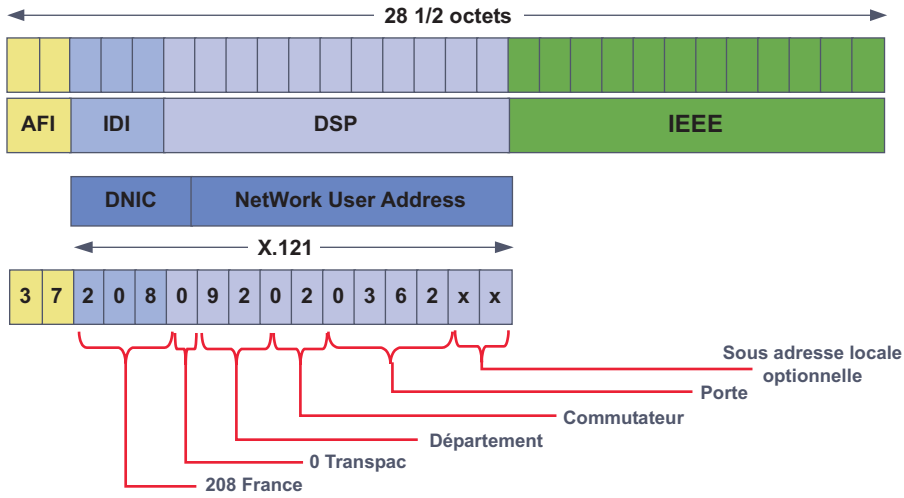


Figure 8.28 L'adressage X.121.

La norme X.121 (figure 8.28) divise l'adresse en deux champs :

– Le **DNIC**, *Data Network Identification Code* ou numéro de réseau, identifie le pays (France 208) et le réseau dans le pays par exemple : Transpac 0. Le tableau de la figure 8.29 fournit, en exemple, quelques numéros de réseau (DNIC) des principaux réseaux publics mondiaux.

– Le **NUA**, *Network User Address*, correspond au numéro de l'abonné dans le réseau. La figure 8.28 représente le format d'adressage utilisé dans le réseau Transpac.

4. En fait, il conviendrait de distinguer l'adresse NSAP qui indique où le service réseau est disponible, de l'adresse SNAP (*SubNetwork Point of Attachement*) qui identifie le point d'accès au réseau physique et constitue la véritable adresse réseau.
5. DCB, Décimal Codé Binaire, dans cette forme de représentation des données, chaque quartet d'un octet code un chiffre décimal, ce qui permet un codage et décodage facile.

Code Pays	Pays	DNIC	Réseau
208 à 212	France	2080 2081 2082 2083	Transpac. NTI. Libre. Administrations.
234 à 238	Grande-Bretagne	2341 2342	IPSS. PSS.
240	Suède	2405	Telepak.
242	Norvège	2422	Norpak.
262	Allemagne	2624	Datex-P.
272	Irlande	2721	PTT.
302 à 307	Canada	3020 3025 3029	Datapac. Teleglobe. Infoswitch.
310 à 329	États-Unis	3106 3110	Tymnet. Telenet.

Figure 8.29 Identification des principaux réseaux dans X.121.

Les techniques d'adressage

Selon les besoins d'identification, on dénombre les cas suivants (figure 8.30) :

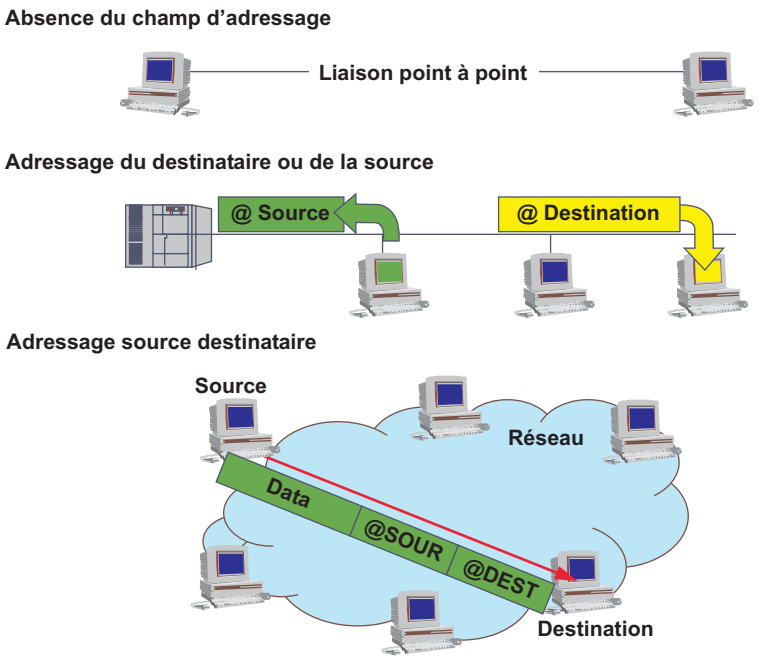


Figure 8.30 Type de relation et adressage.

– Absence de champ d'adresse, seules deux entités peuvent communiquer, c'est le cas d'une liaison en mode point à point où l'adresse est alors inutile.

– Adresse destinataire seule, l'émetteur n'a pas à être connu ou l'est déjà par un autre procédé ;

© Dunod – La photocopie non autorisée est un délit

ce mode d'adressage est utilisé dans les relations du type maître/esclave où le maître est toujours identifié. Seule l'adresse du terminal apparaît dans les échanges, elle désigne celui à qui on parle (adresse destination) ou celui qui répond (adresse source).

– Adresse source uniquement, le récepteur n'est pas identifié, toutes les stations à l'écoute reçoivent les informations (messages de diffusion, broadcast ou mode de contrôle maître/esclave).
– Adresse Source/Destination, cas le plus fréquent, l'adressage est alors dit distribué ou encore global distribué.
– L'adresse est absente du bloc de données, on lui a substitué un label. L'adressage est alors dit en cascade ou adressage de convention. La convention est établie pendant une phase d'initialisation, c'est le cas par exemple de l'attribution du numéro de voie logique dans le mode connecté.

8.4 NOTIONS DE NOMMAGE

8.4.1 Le nommage

La notion de nommage est complémentaire de celle d'adressage, l'un désigne l'objet, l'autre précise sa localisation. Indépendamment qu'il est plus aisé de manipuler des noms que des adresses, l'avantage du nommage est essentiellement de dissocier l'objet de sa localisation géographique. Le déplacement de l'objet nommé est transparent à l'utilisateur. De manière similaire à l'adressage, le nommage utilise deux modes de représentation :

– Le **nommage à plat ou horizontal**, ce type de nommage impose une démarche rigoureuse pour garantir l'unicité d'un nom sur l'ensemble du réseau. NetBios, protocole allégé mis en œuvre dans les réseaux locaux, utilise un nommage à plat.

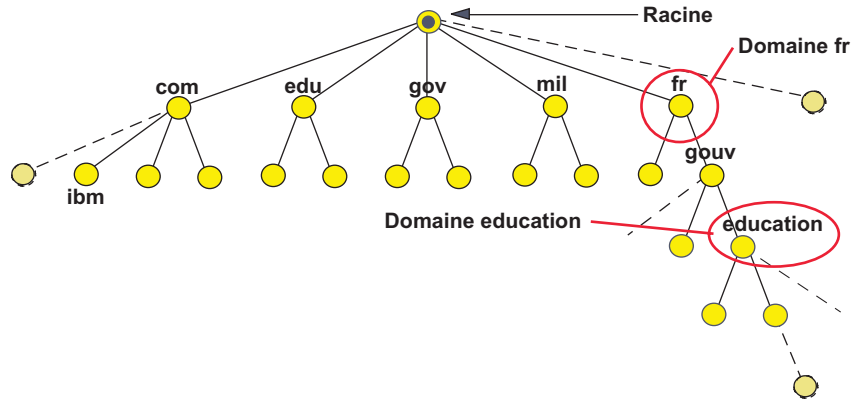


Figure 8.31 Arbre de nommage d'Internet.

– Le **nommage hiérarchique ou arborescent**, plus souple, organise le nommage en domaines. Cette technique autorise une représentation des objets calquée sur l'organisation de l'entreprise. Chaque nœud peut être un domaine dont la gestion peut être confiée à une

autorité particulière. Ce mode de représentation et d'administration convient parfaitement à la gestion d'un annuaire très important comme celui d'Internet (figure 8.31).

8.4.2 Notion d'annuaire

La localisation d'un objet nommé nécessite de mettre en relation son nom et son adresse : résolution de nom. L'association nom/adresse est résolue selon deux techniques (figure 8.32) :

– la consultation d'un fichier local, le nommage est alors dit local ;

– la consultation d'une base de données centralisée ou répartie sur un système local ou des systèmes distants, le nommage est, alors, dit **décentralisé**.

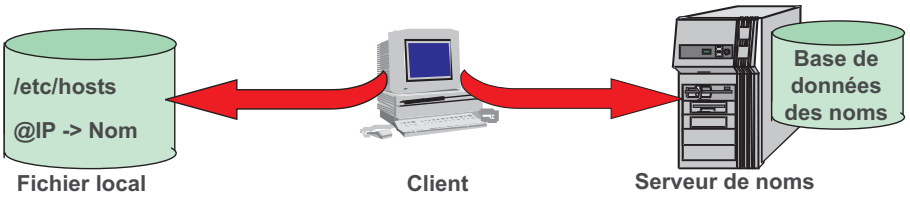


Figure 8.32 Principe de la résolution de nom.

8.5 L'ACHEMINEMENT DANS LE RÉSEAU

8.5.1 Définitions

Acheminer les informations, dans un réseau, consiste à assurer le transit des blocs d'un point d'entrée à un point de sortie désigné par son adresse. Chaque nœud du réseau comporte des tables, dites **tables d'acheminement** couramment appelées **tables de routage**, qui indiquent la route à suivre pour atteindre le destinataire (figure 8.33). En principe, une table de routage est un triplet <Adresse destination>/<Route à prendre>/<Coût>.

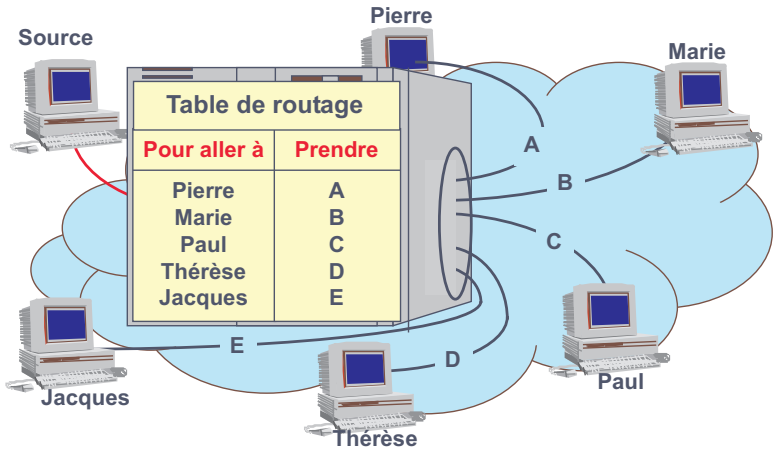


Figure 8.33 Principe d'une table de routage.

© Dunod – La photocopie non autorisée est un délit

Il convient de distinguer la politique d'acheminement qui indique comment est choisie une route, du protocole de routage ou simplement routage qui décrit comment sont construites les tables d'acheminement, c'est-à-dire qu'il spécifie les échanges d'information entre nœuds, le mode de calcul de la route et du coût. Ces deux notions sont souvent confondues.

La politique d'acheminement peut être :

– Déterministe**,** lorsqu'un message arrive dans un nœud, il n'a pas le choix de la route. Une seule route est possible par rapport à la destination. Les tables de routage peuvent être fixées à la configuration du réseau et mises à jour périodiquement par le(s) centre(s) de gestion (gestion centralisée ou décentralisée).
– Adaptative, aucun chemin n'est prédéterminé, le chemin sera fixé au moment du routage en fonction de données sur l'état du réseau (charge, indisponibilité d'un nœud...). La gestion est alors généralement isolée. Le nœud assure la mise à jour de ses tables en fonction de sa connaissance de l'état du réseau.
– Mixte, le choix d'un chemin, adapté à l'état du réseau, est effectué au moment de l'établissement du lien entre les deux entités communicantes. Une fois ce chemin établi, tous les messages d'une même session empruntent le même chemin. La politique est adaptative à l'établissement et déterministe durant le reste de la session. Cette technique est utilisée dans les réseaux en mode orienté connexion. Le circuit virtuel est construit en politique adaptative et les données échangées en politique déterministe.

8.5.2 Les protocoles de routage

Les différents modes de routage

➤ Routage statique ou routage fixe

Le routage statique consiste à construire, dans chaque nœud, une table indiquant, pour chaque destination, l'adresse du nœud suivant. Cette table est construite par l'administrateur du réseau lors de configuration du réseau et à chaque changement de topologie. Simple, le routage fixe assure, même en mode non connecté, le maintien en séquence des informations. Aucun bouclage de chemin n'est à craindre, mais il n'existe pas de solution de secours en cas de rupture d'un lien.

Le routage statique n'est pas optimal, il convient parfaitement aux petits réseaux et aux réseaux dans lesquels il n'existe pas de redondance dans les routes.

➤ Routage par diffusion (de 1 vers n)

L'information est routée simultanément vers plusieurs destinataires ou groupe d'utilisateurs. Le message doit être dupliqué en autant d'exemplaires que de destinataires. Cette technique oblige l'émetteur à connaître tous les destinataires, elle surcharge le réseau. Dans ce cas, on utilise, généralement, un adressage de groupe, chaque nœud n'effectue, alors, que les duplications nécessaires aux sous-groupes ou destinataires finals qu'il dessert (adresse de diffusion).

➤ Routage par inondation (de 1 vers tous)

Dans le routage par inondation, chaque nœud envoie le message sur toutes ses lignes de sortie, sauf celle d'où provient le message. Pour éviter une surcharge du réseau, chaque message com-

porte un compteur de sauts. Le compteur est initialisé à l'émission (nombre de sauts autorisés) et décrémenté par chaque nœud. Le message est détruit quand le compteur de sauts est à zéro. Pour éviter les bouclages, les messages sont numérotés, chaque nœud mémorise cet identifiant et détruit les messages déjà vus.

Ce système est très robuste, il résiste à la destruction de plusieurs lignes et garantit de trouver toujours le plus court chemin ; il est utilisé dans certaines communications militaires et par certains protocoles de routage pour diffuser les informations d'états du réseau.

➤ Routage par le chemin le plus court ou au moindre coût

Dans ce mode de routage, chaque nœud tient à jour des tables indiquant quel est le plus court chemin pour atteindre le nœud destination. Dans ce mode de routage, chaque lien a un coût affecté ou calculé. Ce coût ou métrique peut être exprimé en :

– nombre de sauts ;
– en km, distance réelle ;
– en temps de latence dans les files d'attente ;
– en délai de transmission ;
– fiabilité...

Les algorithmes de routage au moindre coût diffèrent selon la manière dont ils prennent en compte ces coûts pour construire les tables de routage. Dans certains protocoles de routage, un nœud peut maintenir plusieurs tables de routage et ainsi acheminer les données en fonction d'une qualité de service requise.

Le routage au moindre coût

➤ Principe des algorithmes vecteur distance

Dans le routage vecteur distance ou routage de Bellman-Ford *(distance vector routing)*, chaque nœud du réseau maintient une table de routage qui comporte une entrée par nœud du réseau et le coût pour joindre ce nœud. Périodiquement chaque nœud diffuse sa table de routage à ses voisins. Le nœud destinataire apprend ainsi ce que son voisin est capable de joindre.

À réception, le nœud compare les informations reçues à sa propre base de connaissance :

– La table reçue contient une entrée qui n'est pas déjà dans sa propre table, il incrémente le coût de cette entrée du coût affecté au lien par lequel il vient de recevoir cette table et met cette entrée dans sa table. Il a ainsi appris une nouvelle destination.
– La table contient une entrée qu'il connaît déjà. Si le coût calculé (coût reçu incrémenté du coût du lien) est supérieur à l'information qu'il possède, il l'ignore sinon il met sa table à jour de cette nouvelle entrée.

De proche en proche chaque nœud apprend la configuration du réseau et le coût des différents chemins. La convergence des différentes tables peut être assez longue. L'ensemble des schémas de la figure 8.34 illustre ce propos.

À l'initialisation, les routeurs n'ont connaissance que de leur propre existence. La table de routage de chacun ne comporte qu'une entrée, elle indique que le coût pour se joindre est nul (locale). Dans cet exemple, le coût a été fixé à 1 pour tous les liens, le coût retenu par un

© Dunod – La photocopie non autorisée est un délit

nœud correspond donc au nombre de sauts. Périodiquement le contenu des tables est échangé, chaque nœud adresse à son voisin les informations Destination/Coût qu'il connaît.

Au premier échange, le nœud *A* apprend, qu'il peut joindre le nœud *B* en passant par le lien β pour un coût de 0 (contenu de la table du nœud *B* pour l'entrée *B*), coût auquel il convient d'ajouter le coût du transit sur le lien β soit ici 1. *A* n'a pas, en table, d'information concernant *B*, il met sa table à jour. Chaque nœud procède de même. En ne considérant que le nœud *A*, lors du second échange, *A* apprend qu'il peut joindre les nœuds *A*, *B* et *C* en passant par le lien β pour un coût respectif de :

– Pour *A*, de 1 (valeur reçue) + 1 (coût du lien β), soit 2, A a déjà une entrée pour cette destination avec un coût de 0, il conserve l'entrée de moindre coût.
– Pour *B*, de 0 + 1 soit 1, valeur déjà dans sa base connaissance, celle-ci est ignorée.
– Pour *C*, de 1 + 1 soit 2, *A* n'a aucune entrée concernant *C* dans sa table, il ajoute cette valeur.

Le même raisonnement est conduit pour chaque nœud. Les échanges ultérieurs n'apportent aucune connaissance nouvelle. Le routage dans le réseau a atteint sa stabilité (convergence des tables). Le routage par vecteur distance est, avec ses variantes, l'algorithme le plus utilisé. Mais indépendamment du fait que le temps de convergence peut être long, cet algorithme peut conduire à la création de boucle dans le réseau. La figure 8.35 illustre ce propos.

Supposons que le lien entre les nœuds *C* et *B* ne soit plus actif. Le nœud *B* ne reçoit plus d'information en provenance de *C*, il indique qu'il ne peut plus joindre *C* en portant le coût de la route Σ à l'infini. Ne pouvant atteindre cette destination *B* ne diffuse plus cette route. L'instant d'après, *B* reçoit la table de *A*, il apprend ainsi qu'il peut atteindre *C* en passant par β pour un coût de 2 + 1 soit 3, il met à jour sa table. Nous venons de créer une boucle, tout ce que *A* reçoit à destination de *C*, il l'envoie à *B*, tout ce que *B* reçoit à destination de *C*, il l'envoie en *A* !

À l'échange suivant, *A* apprend que joindre *C* en passant par β a maintenant un coût de 3 + 1 soit 4. Il met sa table à jour. À l'échange suivant *B* passe le coût à 5, puis *A* à 6 jusqu'à ce que le coût devienne l'infini. Pour éviter la création de telle boucle, il faut d'une part limiter la valeur de l'infini. Le protocole RIP fixe l'infini à 16, la convergence est alors plus rapide. Et d'autre part, interdire aux nœuds de signaler qu'ils connaissent une destination au routeur par lequel ils l'ont apprise. Cette technique dite de l'horizon coupé ou *Split Horizon* interdit à *A* de signaler à *B* qu'il sait comment aller en *C* en passant par β.

➤ Principe des algorithmes dits à état des liens

Le principal défaut du routage vecteur distance provient du fait que les routeurs n'ont la connaissance d'un changement d'état du réseau que lorsque leur voisin le leur communique, ce qui peut être long. Pour pallier ce défaut, le routage à état des liens (*link state routing*) procède différemment :

– chaque nœud détermine le coût de chaque lien qui lui est raccordé ;
– en cas de modification de cet état, le nœud diffuse cette information dans le réseau, sous la forme (*A*, *B*, c), le lien du nœud *A* vers le nœud *B* a un coût de c ;
– chaque nœud entretien une table où figure pour chaque lien son coût (matrice de coûts). À l'aide de ces informations, chaque nœud peut reconstituer la cartographie complète du réseau ;
– à partir de ces informations, il calcule la table de routage (algorithme de Dijkstra).

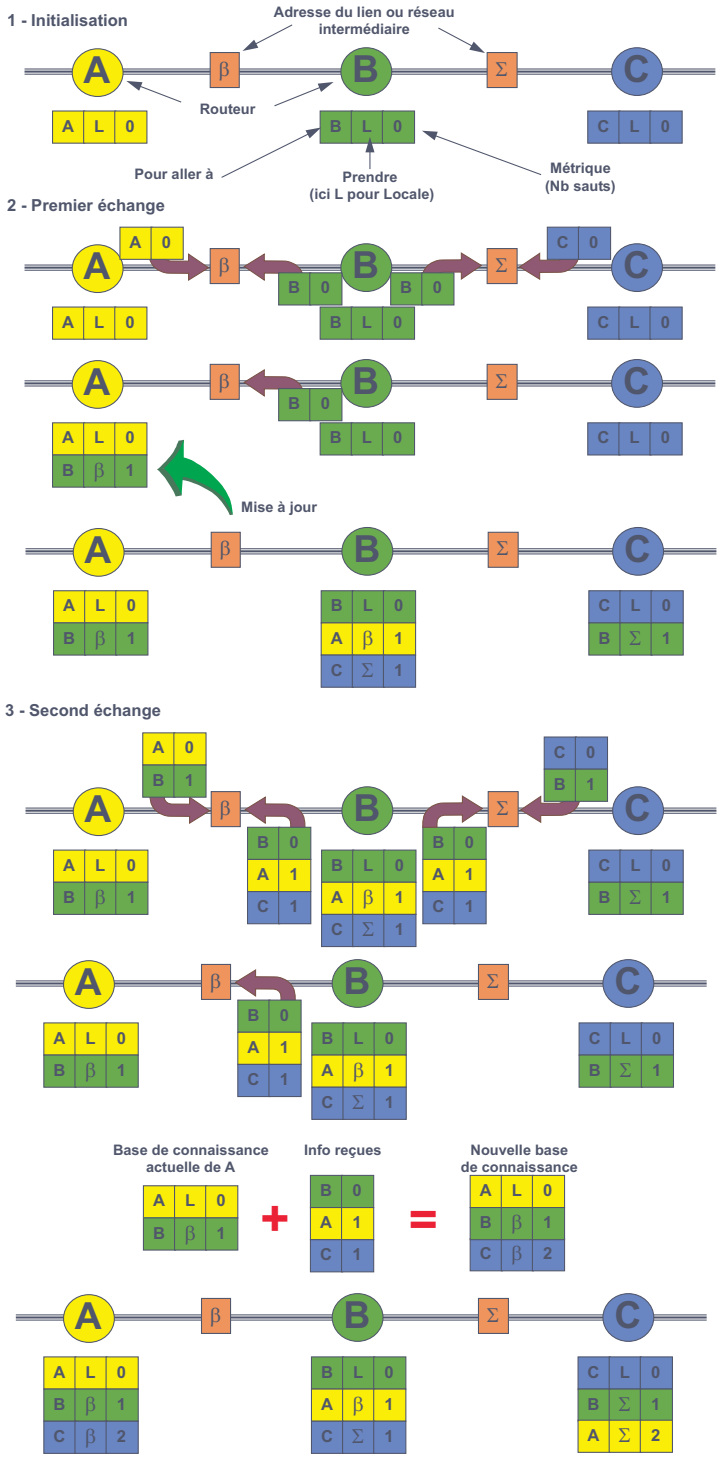


Figure 8.34 Échange des tables en routage vecteur distance.

© Dunod – La photocopie non autorisée est un délit

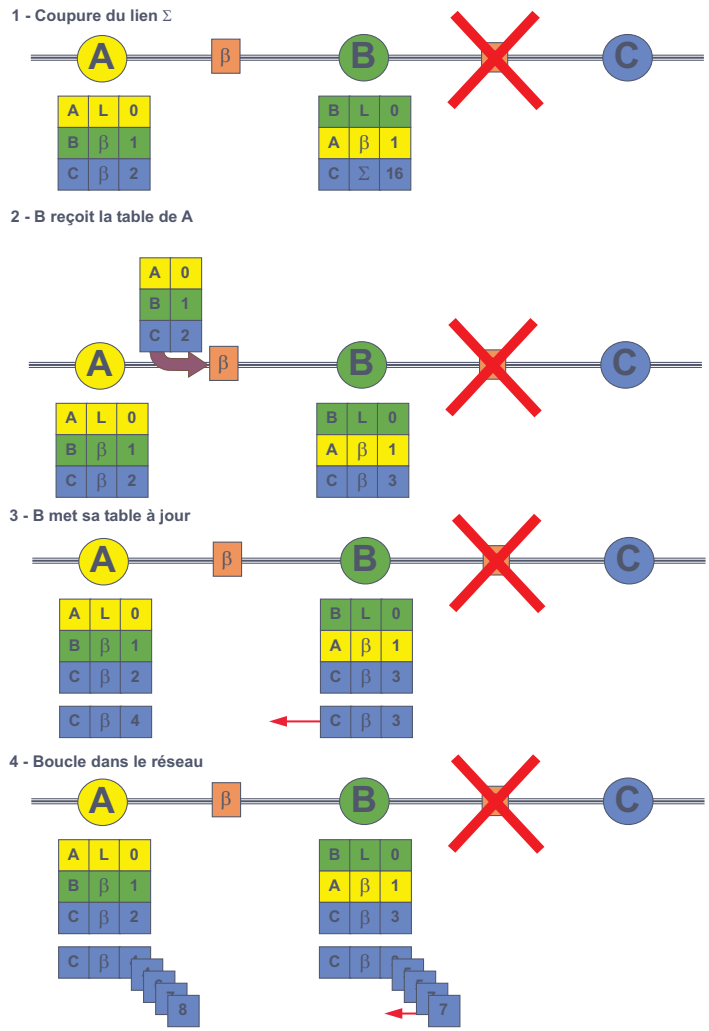


Figure 8.35 Notion d'horizon coupé.

Dans l'exemple de matrice de routage représentée figure 8.36, un coût nul signifie qu'il n'existe pas de lien entre les deux nœuds, la matrice est symétrique c'est-à-dire que nous avons admis que le coût de *A* vers *B* était identique au coût de *B* vers *A*.

$$M = \begin{bmatrix} 0 & 7 & 0 & 0 & 0 & 4 \\ 7 & 0 & 3 & 0 & 2 & 0 \\ 0 & 3 & 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 & 7 & 4 \\ 0 & 2 & 0 & 7 & 0 & 3 \\ 4 & 0 & 0 & 4 & 3 & 0 \end{bmatrix}$$

de \ à	A	B	C	D	E	F
A	0	7	0	0	0	4
B	7	0	3	0	2	0
C	0	3	0	5	0	0
D	0	0	5	0	7	4
E	0	2	0	7	0	3
F	4	0	0	4	3	0

Figure 8.36 Exemple de matrice de coûts.

À titre d'illustration nous allons construire la table de routage du nœud *A* (figures 8.37, 8.38). Dans le tableau de la figure 8.37, les nœuds apparaissent avec la route pour les joindre depuis le nœud précédent et le coût total depuis la racine. Ainsi, « FE, 7 » signifie : la route pour atteindre le nœud *E* en passant par *F* coûte 7 depuis la racine.

Une route possède trois états :

– l'état validé (nœuds grisés figure 8.37), il n'existe, à partir de la racine, aucun autre chemin de moindre coût pour atteindre le nœud ;

– l'état découverte, il s'agit d'une nouvelle route pour joindre le nœud suivant à partir du nœud qui vient d'être validé ;

– l'état attente (nœuds blancs figure 8.37), après avoir été découverte une route peut être rejetée, s'il en existe déjà une de moindre coût pour joindre le nœud extrémité ou être mise en attente.

Routes validées	Routes découvertes		Routes en attente
A,0	AB,7 AF,4	(en attente, ➡) (validée)	AB,7
AF,4	FE,7 FD,8	(en attente ➡) (validée)	AB,7 FD,8
FE,7	EB,9 ED,14	(Fin et validation de AB,7) (Fin et validation de FD,8)	AB,7 FD,8
AB,7	BC,10 BE,9	(en attente, ➡) (Fin, on sait déjà aller en E pour 7)	BC,10
FD,8	DC,13 DF,15	(Fin et validation de BC,10) (Fin, on sait déjà aller en F pour 4)	BC,10
BC,10	CD,15	(Fin, on sait déjà aller en D pour 8)	Vide

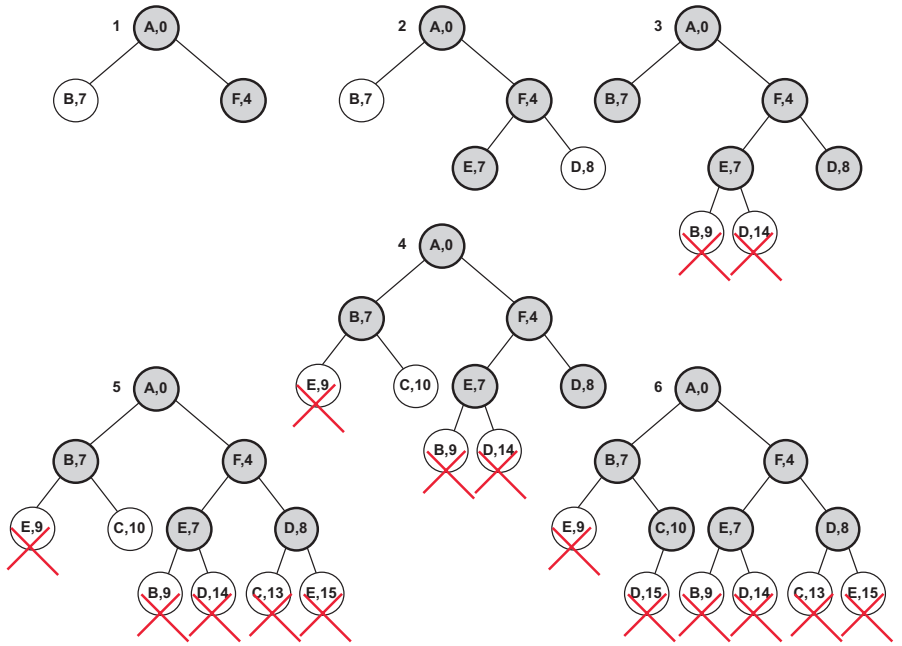


Figure 8.37 Exemple de détermination de la table du nœud A.

© Dunod – La photocopie non autorisée est un délit

La table de routage correspondante est donnée figure 8.38

Nœud destination	Nœud suivant	Coût total
A	Local	0
B	B	7
C	B	10
D	F	8
E	F	7
F	F	4

Figure 8.38 Table de routage du nœud A.

Routage à plat, routage hiérarchique

➤ Notion de domaine de routage

Le routage au moindre coût nécessite la diffusion, à travers le réseau, d'information concernant soit les tables de routage (*vector distance*), soit l'état des liens (*link status*). Ce trafic consomme de la bande passante au détriment des données à écouler. Plus le réseau est grand, plus le trafic de mise à jour est conséquent, plus les tables de routage sont importantes et plus le calcul des routes consomme du temps CPU. En routage hiérarchique (figure 8.39), le réseau est découpé en domaines appelés systèmes autonomes (**AS**, *Autonomus System*). Chaque domaine est identifié, les messages n'appartenant pas au domaine sont éliminés.

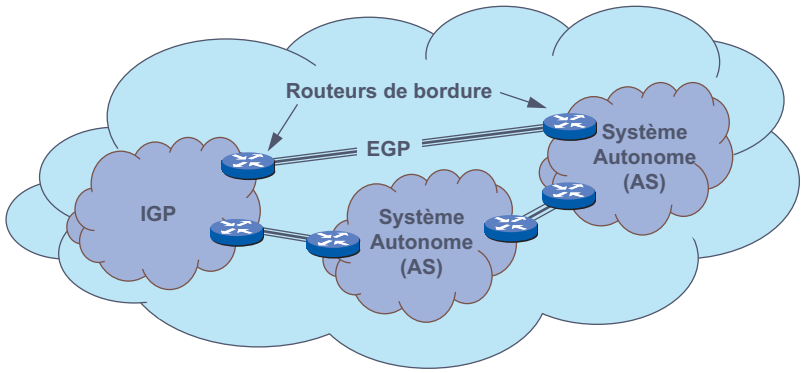


Figure 8.39 Routage hiérarchique.

Ce mode de découpage des réseaux conduit à définir deux familles de protocoles de routage, notamment utilisés dans Internet :

– Les protocoles internes au domaine (**IGP**, *Interior Gateway Protocol*), qui assurent le routage dans le domaine, mais ignorent les nœuds des autres domaines.

– Les protocoles externes au domaine (**EGP**, *External Gateway Protocol*), qui gèrent l'échange d'information entre domaines afin de découvrir la connectivité de chaque domaine.

Chaque domaine est représenté et connu du reste du réseau par un nœud, dit **routeur de bordure**, qui supporte à la fois un protocole intérieur au domaine et un protocole externe au domaine. Chaque domaine est autonome et peut mettre en œuvre un protocole de routage interne différent.

➤ Les principaux protocoles de routage

Les principaux protocoles de routage sont :

– **RIP** (*Routing Information Protocol*, RFC 1058, RIP-2 RFC 1723), du type vecteur distance, RIP est le premier protocole interne. Utilisé dans la communauté Internet, il est aujourd'hui remplacé par OSPF. Malgré une convergence lente et un trafic de gestion important, RIP reste le protocole de routage le plus employé.

– **OSPF** (*Open Short Path First*), d'origine IETF (RFC 2178), protocole interne à état des liens utilisés dans Internet. Pour éviter l'inondation, les informations d'état sont diffusées sur une adresse de multicast réservée à OSPF.

– **IS-IS** (*Intermediate System to Intermediate System*) est le protocole de routage interne de l'ISO (ISO 10589). C'est un protocole à état des liens.

– **IGRP** (*Interior Gateway Routing Protocol*) protocole propriétaire de la société Cisco du type vecteur distance. Cependant, IGRP utilise une métrique construite qui prend en compte le délai d'acheminement, le débit, la fiabilité, la charge du réseau et le **MTU** (*Maximum Transfer Unit*).

– **EGP** (*Exterior Gateway Protocol*, RFC 827) a été le premier protocole externe utilisé dans Internet.

– **BGP** (*Border Gateway Protocol*, RFC 1771) protocole qui définit les échanges à l'intérieur du domaine (iBGP) et entre systèmes de bordure (eBGP).

Routage et commutation

➤ Comparaison

Lorsque la décision d'acheminement est prise en fonction d'une adresse destination (mode datagramme ou paquet d'établissement dans le mode connecté), on parle de **routage**, l'opération est réalisée par un **routeur**. La table d'acheminement est dite **table de routage**. Une décision d'acheminement est prise, pour chaque datagramme, par chacun des routeurs traversés, cette opération peut être longue, elle pénalise l'efficacité du transfert de données (figure 8.40).

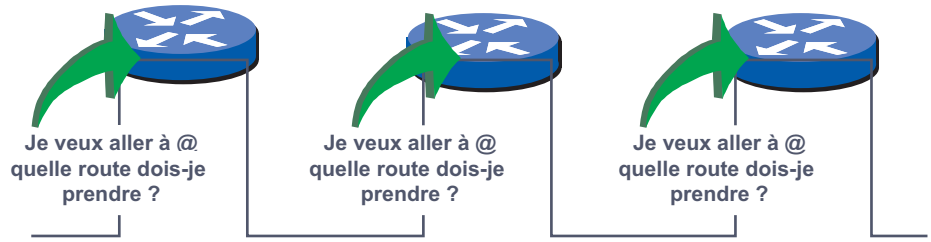


Figure 8.40 Routage à travers le réseau.

Lorsque l'adresse destination n'intervient pas dans le processus de décision d'acheminement, on parle alors de commutation. En mode connecté, une opération de routage est réalisée avant tout envoi de données (phase d'établissement du circuit virtuel, phase 1 de la figure 8.41), les données sont ensuite commutées (phase 2 de la figure 8.41). La décision est prise à partir d'une table, dite **table de commutation**, qui contient un identifiant de flux attribué lors de la phase d'établissement (étiquette) et la voie à prendre.

© Dunod – La photocopie non autorisée est un délit

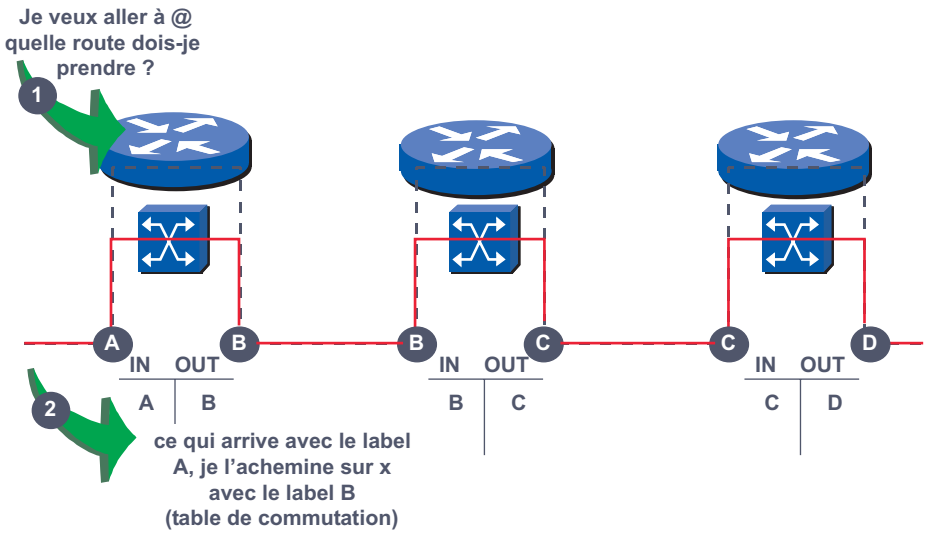


Figure 8.41 Après la phase d'établissement (1), la commutation (2).

La décision de commutation est plus rapide que la décision de routage, les protocoles récents dits à haut débit comme le Frame Relay ou l'ATM (*Asynchronous Transfer Mode*) utilisent ce principe. Devant l'efficacité de ce mode d'acheminement dans les réseaux, l'IETF a défini, pour les protocoles réseaux en mode non connecté, le protocole **MPLS** (*MultiProtocol Label Switching*).

➤ MPLS

MPLS permet un acheminement commuté de datagrammes. À cet effet, un protocole de distribution d'identifiants de route ou labels prédétermine des routes en établissant une correspondance entre une destination IP et un label. En fonction de son adresse destination, chaque datagramme en entrée du réseau se voit affecter, par le routeur de périphérie d'entrée (*Edge Label Switching Router* ou **eLSR**), un identifiant de route (label). Il est ensuite acheminé dans le réseau par rapport à cet identifiant et non plus en fonction de l'adresse destination. Comme dans les réseaux en mode connecté, l'identifiant n'a qu'une valeur locale. Le routeur de sortie supprime le label et achemine le datagramme vers sa destination. L'ensemble forme un réseau MPLS (figure 8.42).

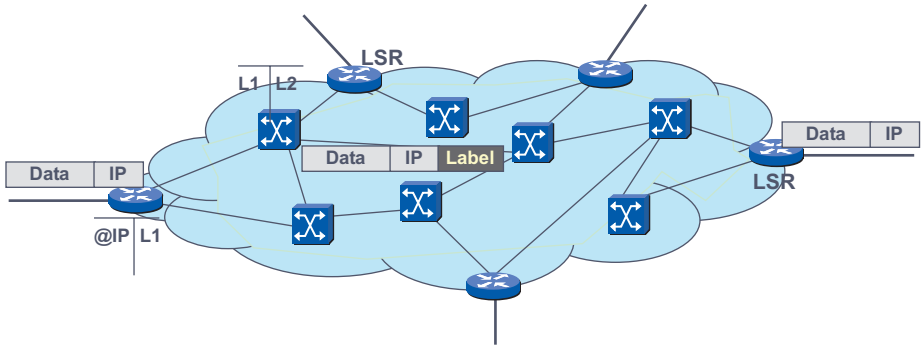


Figure 8.42 Principe de la commutation MPLS.

8.6 ADAPTATION DE LA TAILLE DES UNITÉS DE DONNÉES

8.6.1 Notion de MTU

Lors du transfert d'un bloc de données dans un réseau, chaque élément du réseau (routeur ou commutateur) doit mémoriser les blocs en entrée, les traiter et les délivrer à la file d'attente de sortie. Ces différents traitements nécessitent de la mémoire. La ressource étant limitée, il est nécessaire de fixer une taille maximale aux unités de données admises dans le réseau.

On appelle **MTU** (*Maximum Transfer Unit*) ou unité de transfert maximale, la taille maximale des données admises dans un réseau en-tête compris. Si un bloc a une taille supérieure à la MTU, il devra être fragmenté en plusieurs blocs pour pouvoir être acheminé dans le réseau (figure 8.43).

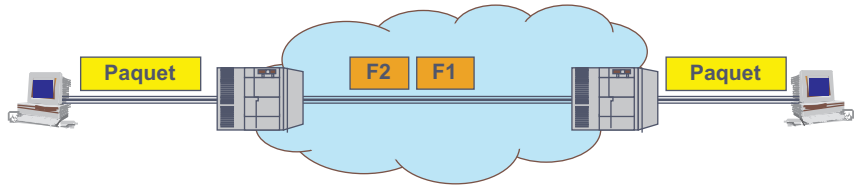


Figure 8.43 Fragmentation d'un paquet.

8.6.2 Segmentation et réassemblage

Dans les réseaux en mode non connecté, les fragments sont susceptibles d'arriver sans respect de l'ordonnancement. Le réassemblage ne peut être réalisé dans le réseau, c'est le destinataire qui devra reconstituer le message (paquet en mode connecté, datagramme en mode non connecté) d'origine. À cette fin, il est nécessaire d'identifier tous les fragments d'un même paquet et de les numéroter pour garantir le réassemblage correct du message initial.

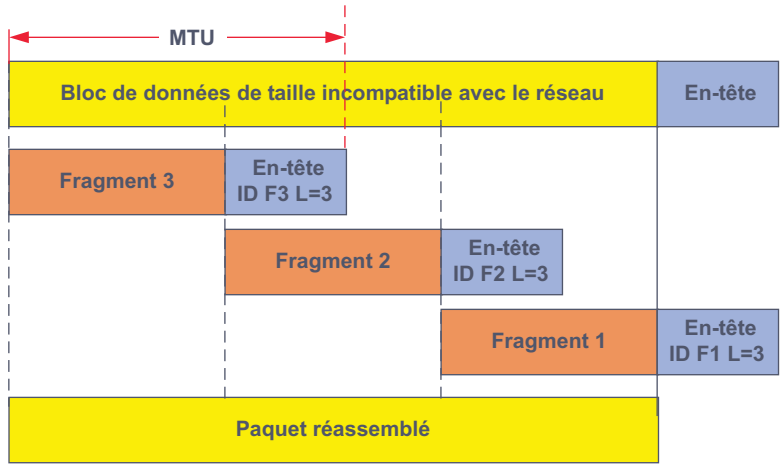


Figure 8.44 Informations de fragmentation en mode non connecté.

Chaque fragment (figure 8.44) comporte les informations nécessaires à son acheminement (adresses). Une donnée d'identification est recopiée dans chaque fragment (ID). Le réassem-

© Dunod – La photocopie non autorisée est un délit

blage nécessite aussi de connaître la longueur totale du paquet d'origine (L) et de disposer d'une information sur l'ordonnancement (F1, F2...). Outre le temps nécessaire aux opérations de fragmentation, en mode non connecté, la perte d'un seul fragment implique la réémission de tout le datagramme. Pour ne pas pénaliser le réseau, les protocoles en mode non connecté offrent généralement des services de découverte de la MTU.

Dans les réseaux en mode connecté, tous les fragments suivent le même chemin, le séquencement est garanti. Dans ces conditions, les informations nécessaires au réassemblage peuvent être réduites à un seul bit (bit *More*, données à suivre). Le bit More est positionné à 1 dans tous les fragments sauf le dernier. Le réassemblage peut être réalisé par le réseau, la fragmentation est alors dite transparente (figure 8.45)

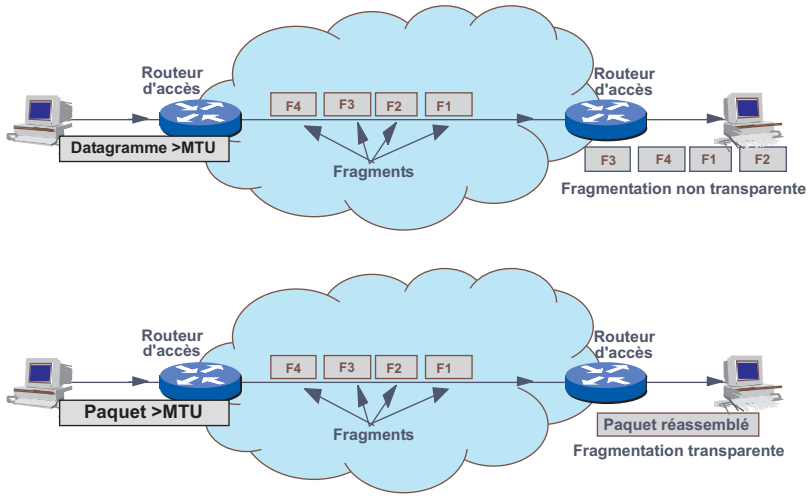


Figure 8.45 Fragmentation transparente et non transparente.

8.7 LA CONGESTION DANS LES RÉSEAUX

8.7.1 Définition

Basé sur un trafic sporadique et aléatoire, le partage statistique des ressources d'un réseau fragilise celui-ci. À une augmentation de trafic soumis, correspond une augmentation du temps d'attente avant traitement dans les nœuds. Vu des sources, le débit diminue, le temps de transit dans le réseau croît (congestion légère). Les paquets retardés peuvent, dans ce cas, ne pas être acquittés dans les délais, ce qui provoque leur retransmission et contribue à augmenter la charge du réseau, plus les paquets ne sont pas acquittés à temps, plus les files d'attente débordent... Le réseau s'effondre, c'est la congestion sévère (figure 8.46). En présence d'une surcharge du réseau, les mécanismes de reprise des protocoles ont tendance à réagir ensemble. L'indépendance des sources n'est plus vraie, la congestion s'installe.

Il est donc nécessaire de mettre en œuvre des mécanismes spécifiques pour d'une part, prévenir l'état de congestion et, d'autre part, si celui-ci apparaît, résoudre l'état de congestion. Ces mécanismes constituent le contrôle de congestion.

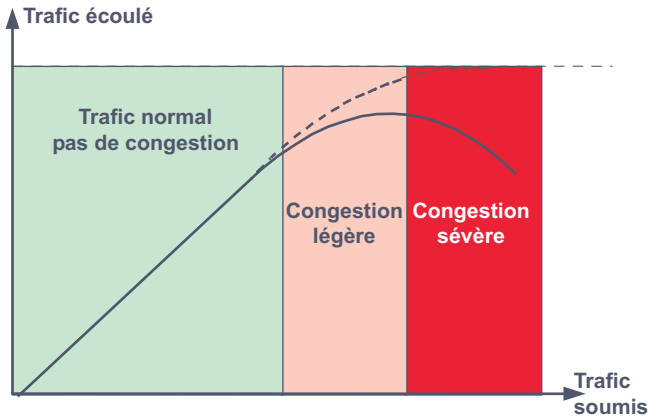


Figure 8.46 Écoulement du trafic dans un réseau.

8.7.2 Les mécanismes de prévention de la congestion

La congestion résulte d'un trafic à écouler supérieur aux capacités du réseau, la solution la plus simple, pour se prémunir contre celle-ci, consiste à ne pas admettre, dans le réseau, plus de trafic que celui-ci est capable d'assimiler. Plusieurs solutions sont envisageables :

– asservir le débit des sources sur les capacités de traitement de chacun des nœuds, c'est le **contrôle de flux** ;

– ne pas admettre plus de trafic dans le réseau que celui-ci n'est capable d'en écouler, c'est le **contrôle d'admission** ;

– éviter la propagation de rafales au cœur du réseau en réalisant un **lissage de trafic**.

Contrôle de congestion et contrôle de flux

Les notions de contrôle de flux et de contrôle de congestion sont différentes. Le contrôle de flux s'intéresse aux échanges entre deux nœuds alors que le contrôle de congestion cherche à limiter le nombre de paquets en transit dans le réseau (figure 8.47). Cependant, en limitant la longueur des files d'attente dans les nœuds intermédiaires, le contrôle de flux participe à la prévention de la congestion.

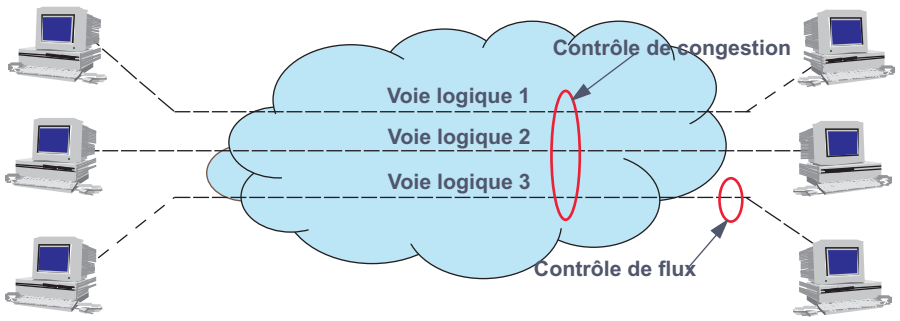


Figure 8.47 Distinction entre contrôle de flux et contrôle de congestion.

© Dunod – La photocopie non autorisée est un délit

Cependant, le contrôle de flux est un mécanisme insuffisant. Compte tenu de la taille de la fenêtre, dans les réseaux haut débit, le contrôle de flux a été abandonné. Il ne subsiste que de bout en bout, c'est-à-dire entre machines d'extrémité.

Contrôle d'admission

Les réseaux en mode circuits sont naturellement protégés contre la congestion. En cas de manque de ressource dans le réseau, la connexion est purement et simplement refusée. Ce mode de prévention se heurte au principe de mutualisation des ressources. Une politique plus souple peut être utilisée : le contrat de service (figure 8.48).

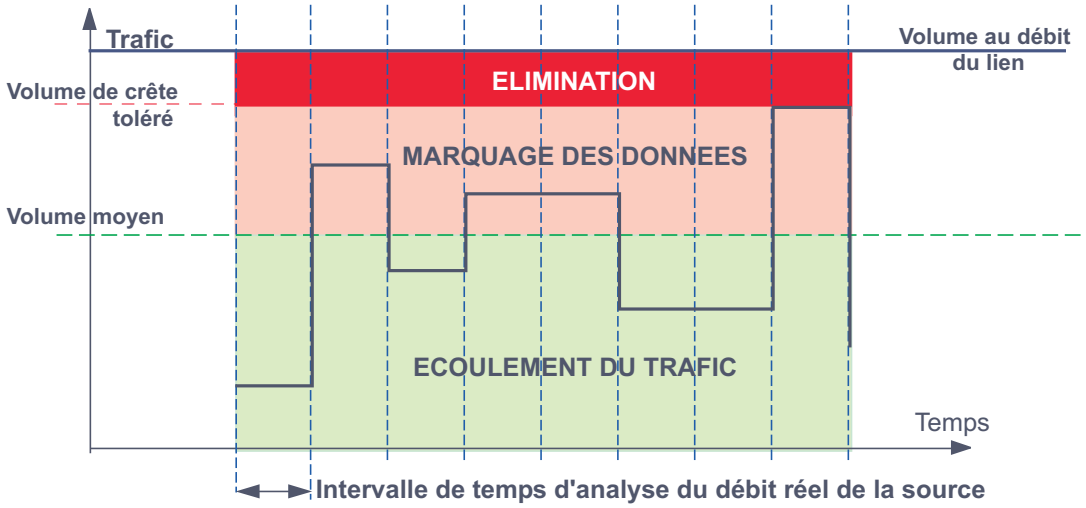


Figure 8.48 Principe du contrat de trafic.

Chaque abonné du réseau spécifie, à l'abonnement ou à la connexion, la description du trafic qu'il va soumettre au réseau (**CAC**, *Connection Admission Control*). Trois zones de fonctionnement peuvent alors être définies. La première correspond à un trafic garanti. Ce trafic, dit **trafic moyen**, est toujours écoulé dans le réseau quel que soit son état. La seconde zone correspond à une zone de tolérance, le trafic soumis est acheminé mais repéré (*Cell tagging*). En cas de congestion, il sera éliminé. Enfin, la troisième zone définit un trafic excédentaire, ou hors contrat, ce trafic est purement et simplement éliminé, il n'est jamais acheminé par le réseau. C'est le nœud d'entrée dans le réseau qui assure le contrôle d'admission.

Le lissage de trafic

Même si chaque source respecte son contrat de service, la congestion peut résulter d'une simultanéité de soumission de rafales par les différentes sources. Pour éviter cet afflux sporadique, on effectue, à l'entrée du réseau, un lissage du trafic (technique du seau percé, *leaky bucket algorithm*). Dans ce système, les données sont mises en file d'attente et délivrées régulièrement. Le mécanisme du seau percé est un mécanisme de prévention utilisé dans ATM, ce n'est pas un mécanisme de résolution, la figure 8.49 illustre ce principe.

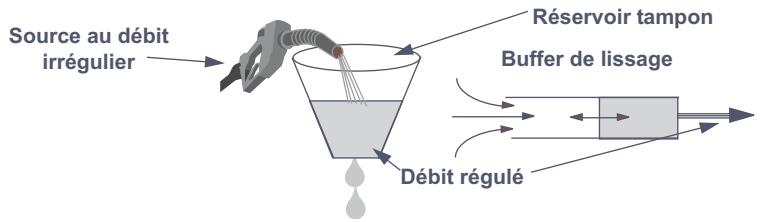


Figure 8.49 Technique du seau percé.

8.7.3 Résolution ou guérison de la congestion

Quels que soient les mécanismes de prévention utilisés, rien ne permet de garantir qu'un état de congestion ne peut apparaître. Plusieurs politiques peuvent être mises en œuvre pour réduire la congestion : ils visent tous à éliminer le trafic en excès. Ces solutions dérivent des principes suivants :

– mettre en attente le trafic excédentaire dans une file d'attente de moindre priorité ;
– identifier le trafic excédentaire (*Cell Tagging*) et l'éliminer en cas de congestion ;
– éliminer tout le trafic ;
– envoyer à la source ou aux sources responsables une demande de ralentissement.

8.8 LA VOIX SUR LES RÉSEAUX EN MODE PAQUETS

8.8.1 Intérêt et contraintes

L'intégration voix/données consiste à transporter la voix sur un réseau en mode paquets en mixant les flux (figure 8.50), elle allège les infrastructures réseaux, puisqu'une seule infrastructure supporte l'ensemble des trafics et optimise l'utilisation du réseau par récupération des silences. La fédération des ressources en une entité unique banalise l'infrastructure locale, simplifie l'administration, permet d'envisager de nouveaux services et, enfin, diminue les coûts, le trafic voix étant facturé au coût de la donnée généralement bien inférieur.

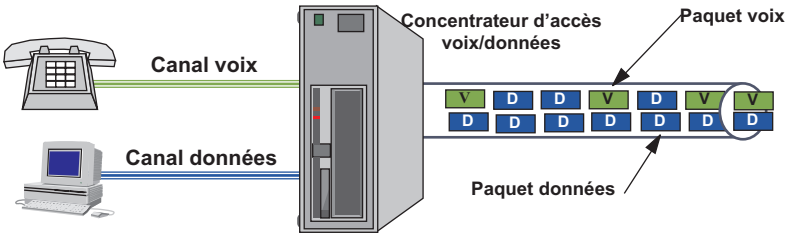


Figure 8.50 Principe des réseaux voix/données.

La voix est un flux temps réel, **isochrone** et *full duplex*. L'adaptation du trafic voix à un réseau de données doit garantir l'intelligibilité et l'interactivité ce qui nécessite :

– de modéliser le flux voix comme un flux de données (paquetisation) ;

© Dunod – La photocopie non autorisée est un délit

– d'adapter les contraintes temps réel aux capacités du réseau (temps de traversée, correction de gigue) ;
– de transformer le flux d'information constant en un flux périodique réduit (compression).

8.8.2 Principe de la paquetisation de la voix

La voix numérisée correspond à un flux de 1 octet toutes les 125 μs, le mode paquets nécessite l'ajout d'information d'acheminement. Il est donc inconcevable de faire sur le réseau 1 octet égal 1 paquet. Par conséquent, il convient d'attendre un certain nombre d'octets, de les rassembler en paquets avant de les acheminer sur le réseau. La paquetisation introduit donc un délai, dit **délai de paquetisation**, valant $N \cdot 125$ μs si le paquet contient N octets (figure 8.51).

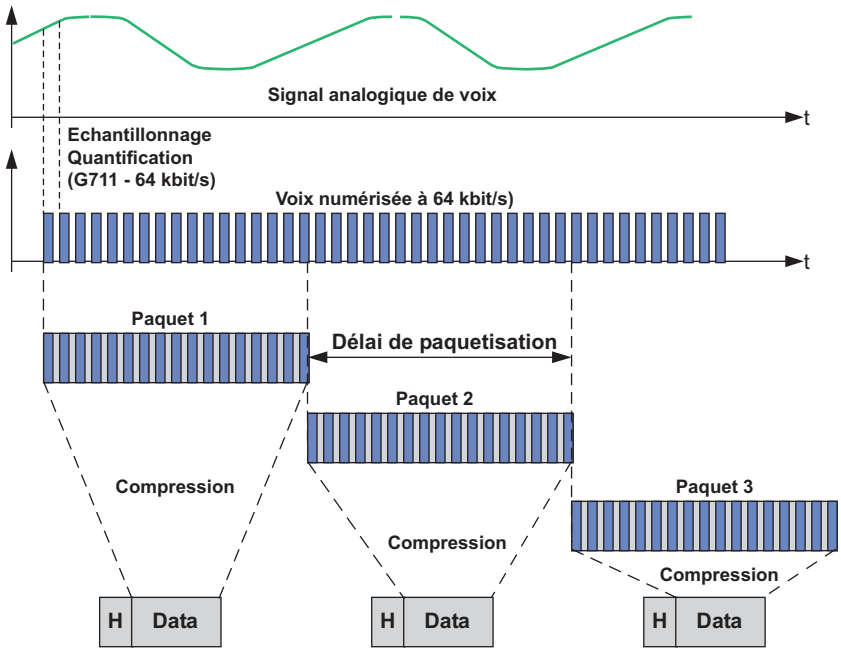


Figure 8.51 Principe de la paquetisation de la voix.

Le délai de paquetisation introduit un retard dans la transmission, la taille du paquet résulte d'un compromis entre l'optimisation de la transmission, le retard introduit et l'influence de la perte d'un paquet sur l'intelligibilité de la voix. La figure 8.52 illustre le bilan temps d'une liaison voix sur un réseau en mode paquets.

Outre les informations de voix, une liaison voix doit assurer le transport des informations de signalisation. Ainsi, une unité de données de voix devra comporter les informations relatives au contenu du paquet (données, voix, signalisation), à l'identification de la communication et éventuellement des informations temporelles.

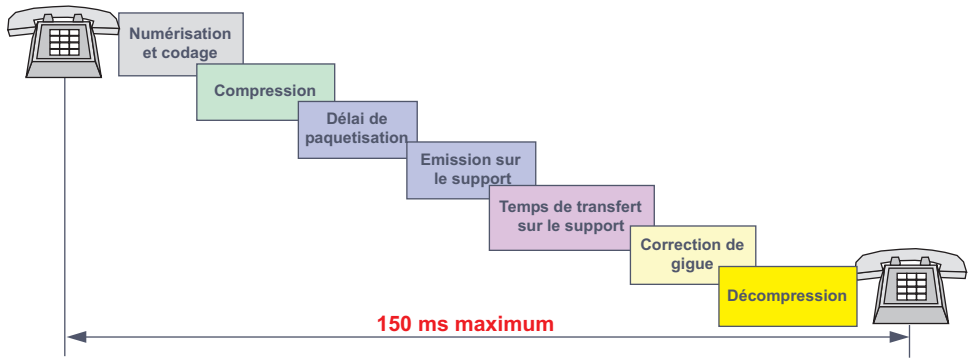


Figure 8.52 Bilan temporel d'une liaison voix.

8.9 CONCLUSION

Les techniques réseaux sont en perpétuelle évolution, le besoin grandissant en bande passante, les contraintes spécifiques à chaque type de flux dopent une recherche très active de la part des constructeurs.

Dans quel cadre doivent se faire les développements, selon quels principes, telles sont les questions auxquelles la normalisation doit répondre pour fournir un cadre de développement et garantir l'interopérabilité des systèmes.

© Dunod – La photocopie non autorisée est un délit

EXERCICES

Exercice 8.1 Évaluation du nombre de liaisons

Déterminez le nombre de liaisons nécessaires à la réalisation d'une interconnexion totale entre 100 équipements.

Exercice 8.2 Table de routage

En reprenant la matrice de routage de la figure 8.36, établissez la table de routage du nœud B et déterminez la topologie du réseau.

Exercice 8.3 Temps de transfert sur un réseau

Deux réseaux LAN de type Ethernet (MTU 1 500 octets) sont interconnectés par un WAN. On vous demande de calculer le temps nécessaire à l'envoi d'un message de 1 480 octets dans les conditions suivantes :

– le protocole réseau nécessite 20 octets d'en-tête (Hn) ;

– le protocole de ligne utilisé sur les liens du WAN rajoute 8 octets d'en-tête (Hl).

et pour les différents modes suivants :

a) En mode commutation de circuits.

b) En mode commutation de messages (dans les mêmes conditions, c'est-à-dire par blocs de 1 500 octets). Le réseau comporte 5 nœuds hors organes d'extrémité.

c) En mode commutation de paquets (mode non connecté, mais les datagrammes seront supposés emprunter le même chemin). Le réseau comporte 5 nœuds hors organes d'extrémité. Faire le calcul pour un MTU de 57, 168, 316 octets. Rappelons que le LAN transmet au routeur des trames de MTU 1 500 octets, c'est le routeur qui a en charge l'adaptation des unités de données au réseau (segmentation).

Le débit des liens sera supposé de 64 kbit/s, les temps de traitement et des stockages intermédiaires seront considérés comme nul. On ne tiendra pas compte des temps d'émission sur les réseaux locaux, seul sera pris en compte le temps de traversée du WAN. Quels commentaires pouvez-vous faire ?

Chapitre **9**

Les architectures protocolaires

Le développement rapide des moyens de calcul et l'importance croissante des systèmes d'information ont engendré la multiplicité des techniques réseaux. La complexité croissante des besoins de communication et la diversité des solutions adoptées ont très vite fait apparaître la nécessité de définir un modèle complet de communication ou **architecture protocolaire réseau**.

Historiquement, chaque grand constructeur avait défini la sienne : SNA (*System Network Architecture*) d'IBM, DSA (*Distributed System Architecture*) de BULL... Ces architectures propriétaires incompatibles entre elles ne permettent pas l'interopérabilité des systèmes. Aussi, convenait-il de définir des techniques de mises en relation en spécifiant une architecture normalisée. C'est ce qu'entreprit l'ISO (*International Standardization Organization*) en définissant une architecture de communication normalisée, couramment appelée modèle de référence ou modèle **OSI** (*Open System Interconnection*)[1].

L'architecture réseau assure à l'utilisateur l'accès aux ressources informatiques et lui procure un service identique que les ressources soient locales ou distantes, pour cela elle doit être transparente à l'utilisateur.

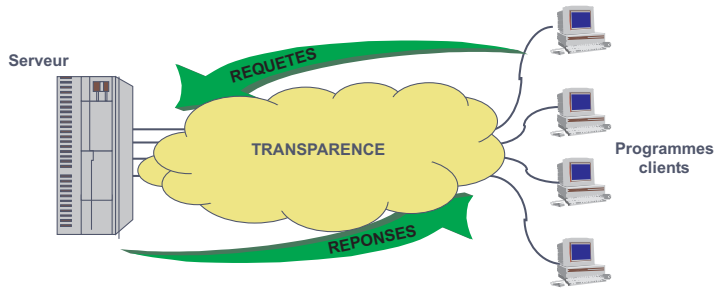


Figure 9.1 L'architecture garantit la transparence.

1. Attention, pour éviter toute confusion due aux traductions, les termes OSI et ISO sont toujours utilisés avec leur appellation anglaise.

Connecter en transparence divers équipements provenant de constructeurs différents pour qu'ils s'échangent des informations nécessite que ceux-ci utilisent, non seulement, des techniques de connexion compatibles (raccordement, niveau électrique...), mais aussi des protocoles d'échange identiques et une sémantique de l'information compréhensible par les partenaires de la communication. Ces problèmes, de nature différente, sont résolus chacun par une solution spécifique. Aussi, pour éviter une description trop complexe, le système a été découpé en entités fonctionnelles appelées couches. Une **couche** est donc un ensemble homogène destiné à accomplir une tâche ou à rendre un service. L'approche en couche garantit une évolutivité facile du système. La prise en compte d'une nouvelle technologie ne remet en cause que la couche concernée. Le modèle de référence est une architecture en couches.

9.1 CONCEPTS DE BASE[2]

9.1.1 Principe de fonctionnement d'une architecture en couches

Considérons le modèle simplifié à 3 couches représenté figure 9.2. Pour communiquer l'application cliente remet à la couche supérieure, ici la couche 3, des données à destination de l'application serveur ainsi que les instructions décrivant le service attendu et celles nécessaires à l'acheminement des données vers l'application serveur. La couche 3 interprète les instructions reçues et confectionne une structure de données à destination de la couche 3 distante, dite **couche homologue**. Cette structure de données est constituée d'une part des informations nécessaires à la couche 3 distante pour traiter ses données appelées en-tête de niveau 3 (H3 pour *Header* de niveau 3) et des données elles-mêmes ; l'ensemble forme une unité de données de niveau N. Les règles d'échange entre données de même niveau constituent un protocole de niveau N.

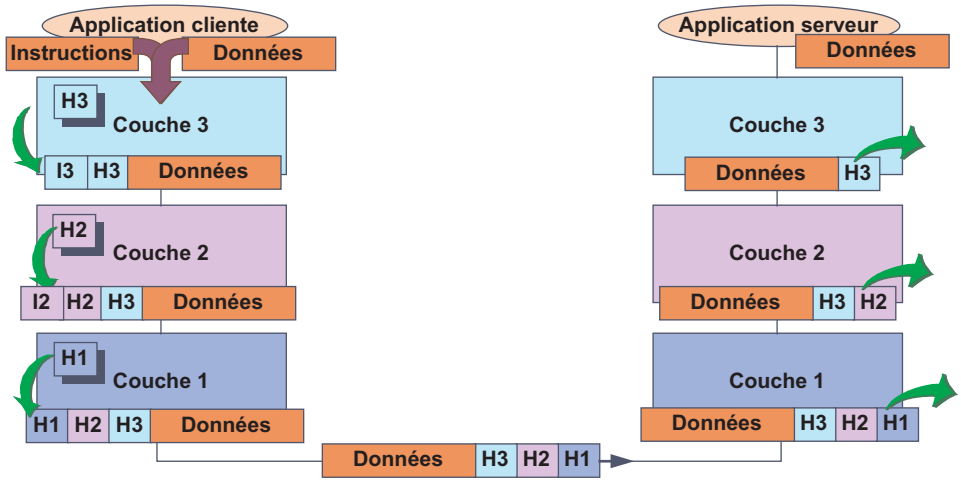


Figure 9.2 Principe général de fonctionnement d'un modèle en couches.

2. Tous les modèles architecturaux utilisent les mêmes principes. Dans les paragraphes qui suivent nous emploierons, pour décrire ces principes, la terminologie utilisée par l'ISO pour le modèle de référence.

Puis, la couche 3 remet cette unité de données et des instructions (I3) à la couche inférieure qui procède de même... Enfin les données sont émises vers le réseau. En réception la couche la plus basse extrait l'en-tête protocolaire (H1), l'interprète, et remet les données à la couche supérieure qui procède de même jusqu'à remise des données à l'application distante.

9.1.2 Terminologie

Protocole et service

L'échange précédent, illustré figure 9.2, montre deux types de dialogues (figure 9.3) :

– un dialogue vertical qui correspond au transfert d'informations d'une couche à une autre (couches adjacentes), ce dialogue est réalisé à l'aide de **primitives de service** ;

– un dialogue horizontal qui par l'intermédiaire de messages échangés (protocole) à travers le réseau transfère, entre couches distantes de même niveau (**couches homologues**), les données d'un système à un autre. Ce dialogue constitue le **protocole de niveau N**.

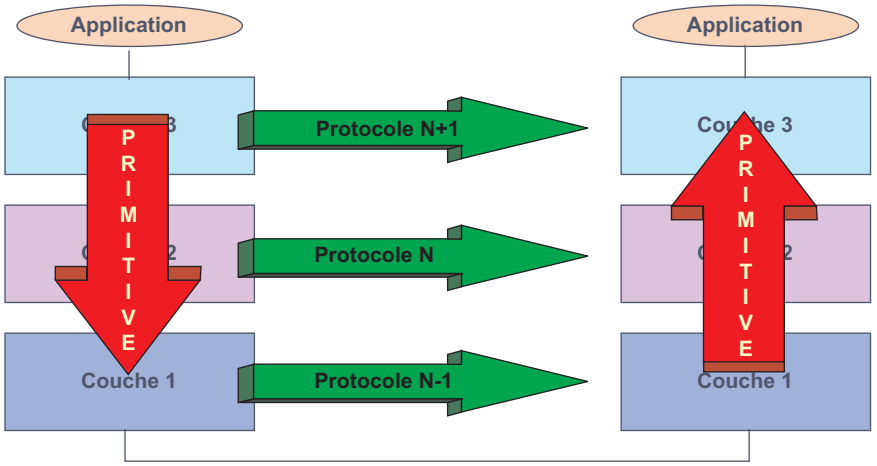


Figure 9.3 Protocoles et primitives de service.

L'encapsulation de données

La couche (N + 1) a requis les services de la couche N, à l'aide d'une primitive de service de niveau N, pour que celle-ci lui rende le service de niveau N (figure 9.4). Peu importe à (N + 1) de savoir comment ces services sont rendus. L'unité de données protocolaire de niveau (N + 1), données et en-tête, est transportée dans une unité de données de niveau N (protocole N). Les données de niveau (N + 1) sont dites **encapsulées** dans le protocole N, on parle aussi de **tunnel de niveau N** .

Point d'accès au service (SAP)

Une couche (N) procure le service (N) au moyen d'un protocole de niveau (N). Le service de la couche (N) est fourni par une entité de niveau (N) qui est une occurrence d'un élément actif de la couche (N). La figure 9.5 illustre ce principe.

© Dunod – La photocopie non autorisée est un délit

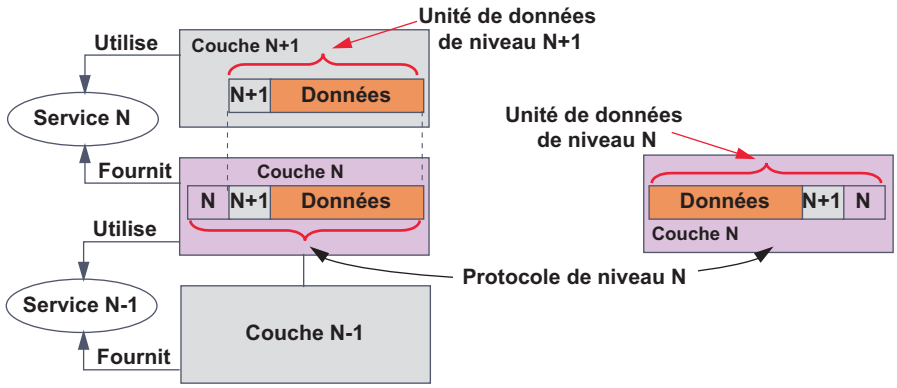


Figure 9.4 Service et encapsulation de données.

Les services de la couche (N) sont offerts par une entité de niveau N et accessibles via une interface désignée par un identificateur ou point d'accès au service (**SAP**, *Service Access Point*). Un SAP ne peut être rattaché qu'à une seule entité, mais une même couche peut mettre en œuvre plusieurs occurrences de l'entité de niveau (N).

Le dialogue OSI est un dialogue entre entités homologues distantes via une mise en relation ou connexion de niveau (N – 1).

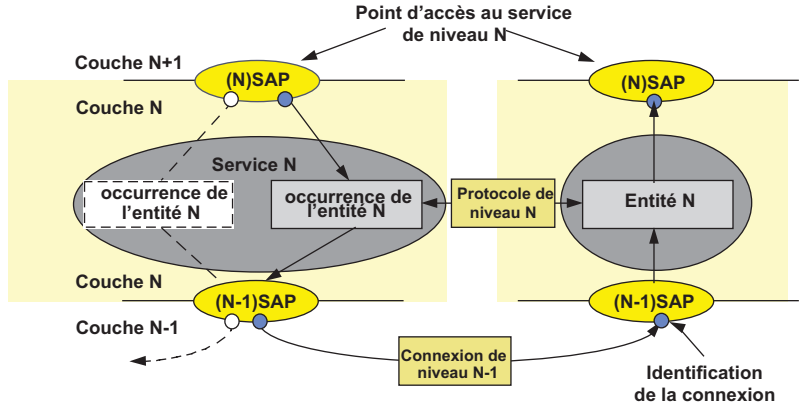


Figure 9.5 L'identification des services.

Les unités de données manipulées

Les données manipulées par une couche et envoyées à l'entité homologue constituent une unité de données (*Data Unit*). La couche de niveau (N + 1), utilisatrice des services de niveau (N), adresse à la couche (N), des unités de données de service notées (N)SDU[3] (*Service Data Unit*). Pour la couche (N), les données entrantes sont considérées comme utilisatrices du service (N).

3. Les notations OSI utilisent, pour désigner les couches, les notations suivantes :
– (N) SDU désigne une SDU de niveau (N) générique ;
– N_SDU désigne une SDU d'un niveau particulier, ici le niveau 3 (Network).

La couche N ajoute aux données reçues (SDU) des informations de service nécessaires à la couche N homologue pour que celle-ci traite et délivre correctement les données à sa couche (N + 1) distante. Ces informations de protocole constituent le (N)**PCI** (*Protocol Control Information*). Les données sont acheminées vers l'entité homologue via une connexion de niveau (N – 1). La couche N distante recevant la (N)SDU extrait le (N)PCI, l'interprète et délivre les données (N)SDU à la couche (N + 1) ; ces données deviennent alors la (N + 1)PDU. La figure 9.6 illustre ce mécanisme.

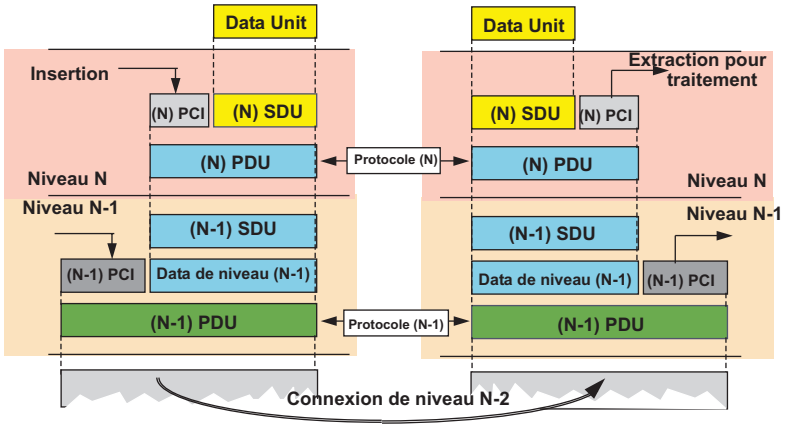


Figure 9.6 Modèle général d'une couche.

Ainsi, chaque couche ajoute (ou extrait) un en-tête (*Header*), spécifique au protocole utilisé, permettant de traiter les données. Cet en-tête contient toutes les informations nécessaires au traitement distant de l'unité de données : l'identifiant de la connexion, l'adresse du destinataire, les compteurs de contrôle de l'échange...

Contrôle de l'interface

Lors de l'invocation d'un service de niveau (N), le niveau (N + 1) fournit un ensemble d'informations nécessaires au traitement correct de l'unité de données. Une partie de ces informations est utilisée pour construire le PCI, comme, par exemple les informations concernant l'adressage, le niveau de priorité demandé... L'autre est à l'usage exclusif de l'entité de niveau N, elle précise le traitement qui doit être opéré localement sur les données. Ces informations de contrôle de l'interface (**ICI** , *Interface Control Information*) sont annexées à la SDU pour former une unité de données de contrôle de l'interface (**IDU**, *Interface Data Unit*). L'ICI à usage exclusif de la couche N n'est pas transmis. La figure 9.7 illustre ce propos.

Protocole en mode point à point et de bout en bout

La communication entre deux systèmes peut être directe ou se réaliser à travers un ou plusieurs relais (sous-réseau réel de transport ou autre moyen d'interconnexion). Cette approche conduit à définir deux types de dialogue (figure 9.8) :

– Un dialogue entre les systèmes d'extrémité et le relais : dialogue en mode point à point.

– Un dialogue entre les systèmes d'extrémité : dialogue de bout en bout.

© Dunod – La photocopie non autorisée est un délit

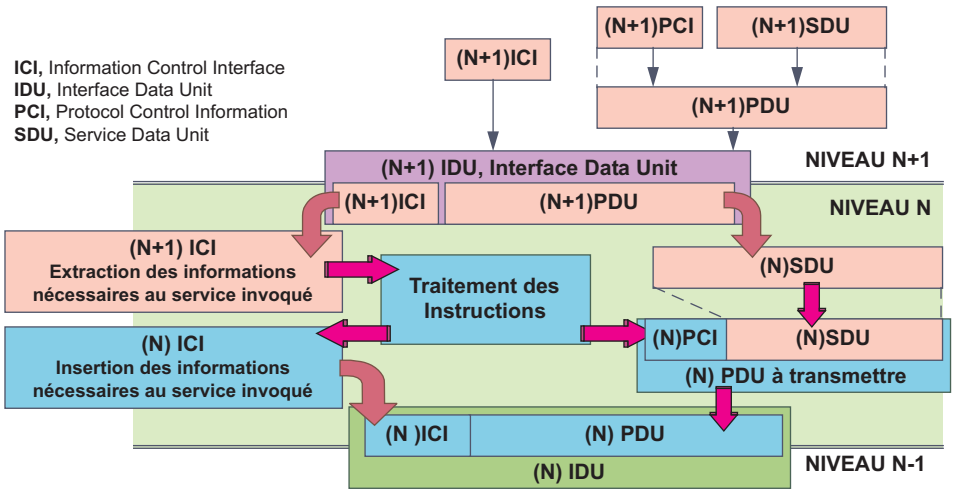


Figure 9.7 Le contrôle de l'interface.

Les protocoles de point à point assurent le transport de l'information dans le sous-réseau réel de transport, ils assurent notamment le contrôle du lien, le contrôle et éventuellement la reprise sur erreur, l'adressage et l'acheminement. Les protocoles en mode point à point peuvent être en mode orienté connexion ou en mode non connecté.

Les protocoles de bout en bout doivent essentiellement vérifier l'intégrité, au sens large, des informations remises aux applications et organiser le dialogue. Les protocoles de bout en bout sont généralement en mode orienté connexion.

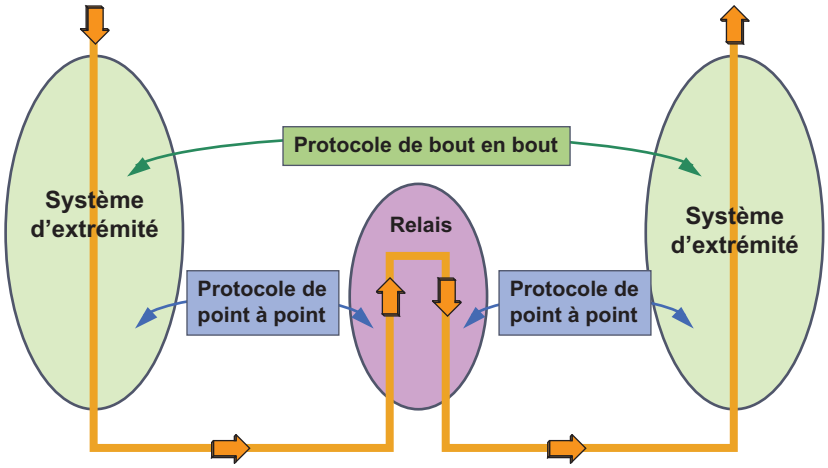


Figure 9.8 Protocole en mode point à point ou de bout en bout

9.2 ORGANISATION DU MODÈLE DE RÉFÉRENCE

9.2.1 Concepts ayant conduit à la modélisation

Définition

Au sens du modèle OSI, modèle pour l'interconnexion des systèmes ouverts, on appelle système réel l'ensemble constitué d'un ou plusieurs ordinateurs, logiciels, périphériques associés

et opérateurs humains capables d'effectuer des traitements informatiques et de s'échanger des informations (normes ISO IS7498, NF 27498). Un système est dit ouvert si les communications entre les divers constituants s'effectuent conformément au modèle de référence (OSI).

Principes ayant guidé à la détermination des couches

La nécessité d'identifier des fonctions élémentaires distinctes, mais participant au processus de communication, a conduit à étudier un modèle structuré en couches. La définition des différentes couches descriptives du modèle respecte les principes suivants :

– Ne pas créer plus de couches que nécessaire, pour que le travail de description et d'intégration reste simple, ce qui conduit à regrouper les fonctions similaires dans une même couche.

– Créer une couche chaque fois qu'une fonction peut être identifiée par un traitement ou une technologie particulière mise en jeu.

– Créer une couche là où un besoin d'abstraction de manipulation de données doit être distingué.

Une interface sera créée à la frontière de chaque couche. Les figures 9.9 et 9.10 illustrent le principe de la structuration du système. Chaque couche (N) fournit les services (N) aux entités (N + 1) de la couche (N + 1). Chaque couche échange des unités de données (*Data Unit*) avec la couche correspondante sur l'entité distante (homologue) à l'aide d'un ensemble de règles (protocole) en utilisant pour cela les services de la couche inférieure.

Couches hautes, couches basses

Deux fonctions essentielles peuvent être distinguées pour assurer l'interfonctionnement d'applications informatiques à travers un réseau (figure 9.9).

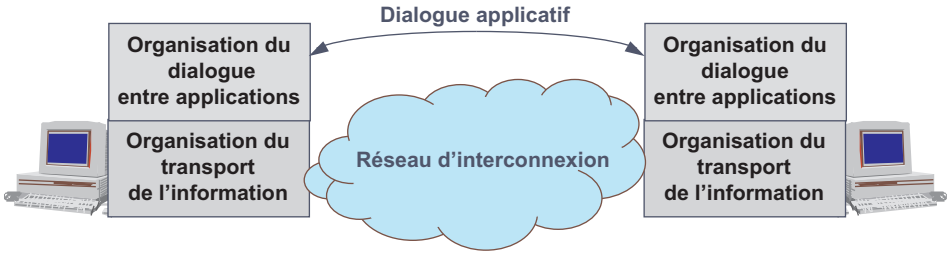

Dialogue applicatif
Organisation du dialogue entre applications
Organisation du transport de l'information
Réseau d'interconnexion
Organisation du dialogue entre applications
Organisation du transport de l'information

Figure 9.9 Interfonctionnement des applications.

Il faut, d'une part garantir un transport fiable des informations à travers le réseau, et d'autre part organiser le dialogue entre les applications distantes (dialogue applicatif). Le modèle devant masquer à l'utilisateur la répartition physique des ressources et offrir les mêmes performances pour des ressources locales ou distantes.

Cet aspect conduit à spécifier deux ensembles de couches aux fonctionnalités spécifiques (figure 9.10) :

– les **couches hautes** essentiellement chargées d'assurer l'interfonctionnement des processus applicatifs distants, ces couches sont dites orientées application ;

– les **couches basses** destinées à fournir aux couches hautes un service de transport fiable de

© Dunod – La photocopie non autorisée est un délit

données, déchargeant les couches hautes de la gestion de tous les mécanismes de localisation et de transfert d'information à travers un ou plusieurs systèmes relais, ces couches sont dites orientées transport (ou transfert).

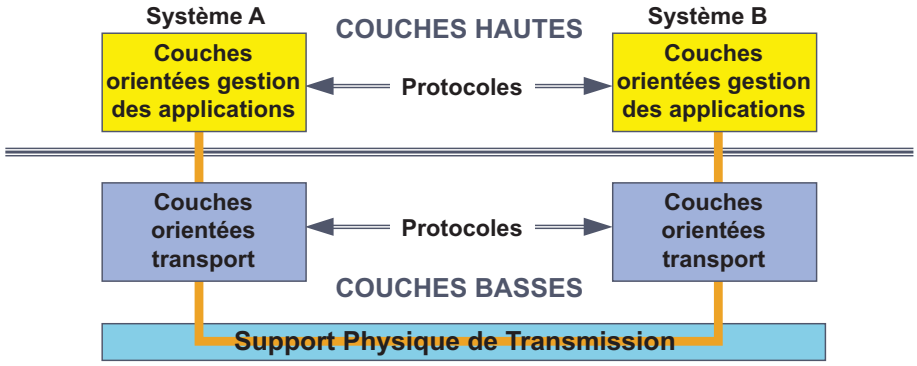


Figure 9.10 Spécification en deux ensembles de couches.

Les couches basses garantissent aux couches hautes que le transfert d'information se réalise correctement. Il est donc nécessaire que la dernière couche basse destination s'assure, avant de délivrer les données aux couches applicatives, que celles-ci sont correctes (contrôle de bout en bout). Les autres couches inférieures n'effectuent qu'un transfert de proche en proche entre systèmes. Les couches hautes n'assurent, globalement, que l'organisation des échanges et fournissent les mécanismes nécessaires à assurer l'interfonctionnement de une ou plusieurs applications distantes.

9.2.2 Description du modèle de référence

Définition des couches

Pour réaliser une communication à travers un ou plusieurs systèmes intermédiaires (relais) il faut (figure 9.11) :

- relier les systèmes par un lien physique (couche PHYSIQUE) ;
- contrôler qu'une liaison peut être correctement établie sur ce lien (couche LIAISON) ;
- s'assurer qu'à travers le relais (réseau) les données sont correctement acheminées et délivrées au bon destinataire (couche RÉSEAU) ;
- contrôler, avant de délivrer les données à l'application que le transport s'est réalisé correctement de bout en bout (couche TRANSPORT) ;
- organiser le dialogue entre toutes les applications, en gérant des sessions d'échange (couche SESSION) ;
- traduire les données selon une syntaxe de présentation aux applications pour que celles-ci soient compréhensibles par les deux entités d'application (couche PRÉSENTATION) ;
- fournir à l'application utilisateur tous les mécanismes nécessaires à masquer à celle-ci les contraintes de transmission (couche APPLICATION).

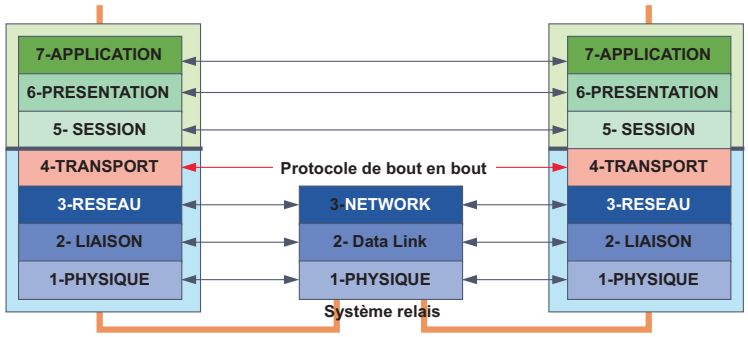


Figure 9.11 Le modèle de référence.

C'est ainsi, qu'après de nombreux débats, le modèle de référence a été défini en 7 couches (compromis entre 6 et 8 !). Le modèle de référence (figure 9.11) ne définit pas seulement des fonctionnalités de couche mais précise aussi la dénomination des unités de données (figure 9.13). La figure 9.12 détaille les fonctionnalités de chacune des couches composant le modèle.

COUCHES	FONCTIONS
NIVEAU 1 **Couche Physique** ***Physical Layer***	La couche physique assure un transfert de **bits** sur le canal physique (support). À cet effet, elle définit les supports et les moyens d'y accéder : spécifications mécaniques (connecteur), spécifications électriques (niveau de tension), spécifications fonctionnelles des éléments de raccordement nécessaires à l'établissement, au maintien et à la libération de la ligne. Elle détermine aussi les moyens d'adaptation (ETCD).
NIVEAU 2 **Couche Liaison de données** ***Data Link Layer***	La couche liaison assure, sur la ligne, un service de transfert de blocs de données (**trames**) entre deux systèmes adjacents en assurant le contrôle, l'établissement, le maintien et la libération du lien logique entre les entités. Les protocoles de niveau 2 permettent, en outre, de détecter et de corriger les erreurs inhérentes aux supports physiques.
NIVEAU 3 **Couche Réseau** ***Network Layer***	La couche réseau assure, lors d'un transfert à travers un système relais, l'acheminement des données (**paquets**) à travers les différents nœuds d'un sous-réseau (routage). Les protocoles de niveau 3 fournissent les moyens d'assurer l'acheminement de l'appel, le routage, le contrôle de congestion, l'adaptation de la taille des blocs de données aux capacités du sous-réseau physique utilisé. Elle offre, en outre, un service de facturation de la prestation fournie par le sous-réseau de transport.
NIVEAU 4 **Couche Transport** ***Transport Layer***	La couche transport est la couche pivot du modèle OSI. Elle assure le contrôle du transfert de bout en bout des informations (**messages**) entre les deux systèmes d'extrémité. La couche transport est la dernière couche de contrôle des informations, **elle doit assurer aux couches supérieures un transfert fiable quelle que soit la qualité du sous-réseau de transport utilisé**.
NIVEAU 5 **Couche Session** ***Session Layer***	La couche session gère l'échange de données (**transaction**) entre les applications distantes. La fonction essentielle de la couche session est la synchronisation des échanges et la définition de points de reprise.
NIVEAU 6 **Couche Présentation** ***Presentation Layer***	Interface entre les couches qui assurent l'échange de données et celle qui les manipule, cette couche assure la mise en forme des données, les conversions de code nécessaires pour délivrer à la couche supérieure un message dans une syntaxe compréhensible par celle-ci. En outre, elle peut, éventuellement, réaliser des transformations spéciales, comme la compression de données.
NIVEAU 7 **Couche Application** ***Application Layer***	La couche application, la dernière du modèle de référence, fournit au programme utilisateur, l'application proprement dite, un ensemble de fonctions (entités d'application) permettant le déroulement correct des programmes communicants (transferts de fichiers, courrier électronique...).

Figure 9.12 Brève description des fonctionnalités de chaque couche.

© Dunod – La photocopie non autorisée est un délit

Mécanismes élémentaires

➤ L'encapsulation

Chaque couche du modèle insère un en-tête de protocole PCI. La figure 9.13, où le symbole H*x* représente l'en-tête (*Header*) de niveau, illustre ces mécanismes.

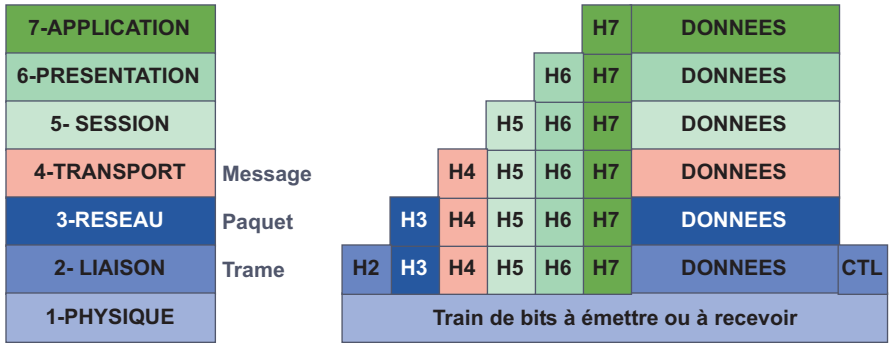


Figure 9.13 L'encapsulation des données dans le modèle OSI.

La couche liaison de données ajoute un champ supplémentaire qui contient les informations nécessaires au contrôle (CTL) de la transmission (**FCS**, *Frame Check Sequence*). Le mécanisme d'encapsulation est illustré par la figure 9.13.

➤ Primitives de service

Les services offerts par la couche (N) sont invoqués par la couche (N + 1) à l'aide de primitives de service de niveau (N). Par exemple, en mode connecté (figure 9.14), quatre primitives sont utilisées pour offrir un service : demande (*request*), indication (*indication*), réponse (*response*), confirmation (*confirm*). En mode non connecté, seules les primitives demande (*request*) et indication (*indication*) sont exploitées.

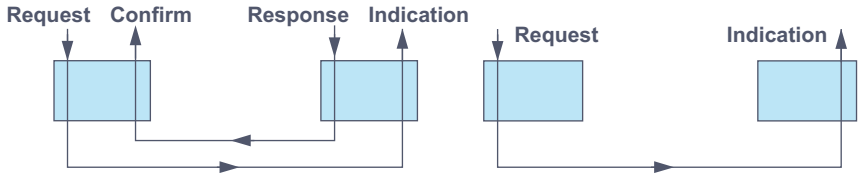


Figure 9.14 Les primitives de service.

Mécanismes pouvant être mis en œuvre dans une couche

➤ L'adaptation de la taille des unités de données

Les unités de données, manipulées par les différentes couches ou par les systèmes intermédiaires, ne sont pas forcément de taille compatible avec les capacités de ces systèmes. Différents mécanismes peuvent alors être utilisés (figure 9.15).

La segmentation consiste à diviser une unité de données du service (N) en plusieurs unités de données de protocole (N). L'entité correspondante doit être capable d'assurer le réassemblage afin de reconstituer la SDU d'origine.

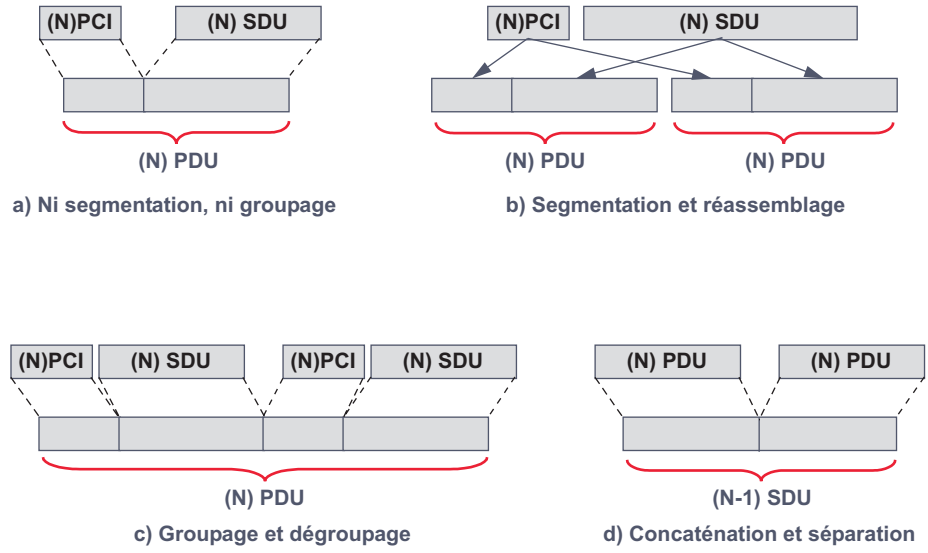


Figure 9.15 L'adaptation de la taille des unités de données.

Le groupage réunit en une seule PDU de niveau (N) plusieurs unités de données de service. Chaque unité possède son propre en-tête.

La concaténation procède de la même manière, plusieurs PDU de niveau N sont associées pour former une seule SDU de niveau N – 1.

➤ Le multiplexage et l'éclatement des connexions

Le multiplexage (figure 9.16) consiste pour une couche à prendre en charge plusieurs connexions de niveau (N) sur une seule connexion de niveau (N – 1). Alors que l'éclatement permet à la couche (N) d'utiliser plusieurs connexions (N – 1).

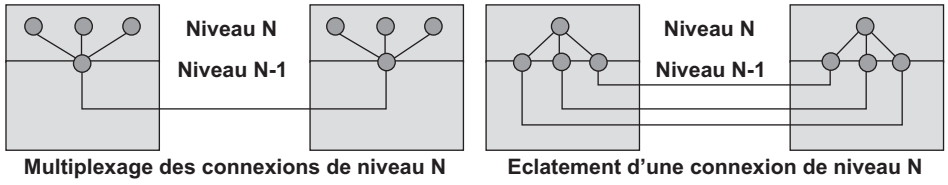


Figure 9.16 Multiplexage et éclatement.

➤ Le contrôle de flux

Cette technique, déjà évoquée, assure une cadence de délivrance des données compatibles avec les capacités de traitement entre couches adjacentes (contrôle de flux à l'interface) ou entre couches homologues (contrôle de flux entre systèmes).

➤ Le maintien en séquence

Cette fonction garantit que les données remises à une couche (N) sont dans le même ordre que celles émises par la couche (N) distante. Le maintien en séquence n'est pas obligatoirement garanti par toutes les couches. La couche chargée de cette fonction doit être capable de mémoriser les données reçues hors séquence et les ordonner avant de les délivrer en séquence

© Dunod – La photocopie non autorisée est un délit

à la couche supérieure. La fenêtre de réception représente, en nombre d'unités de données, la capacité de mémorisation et de réordonnancement de la couche. Le maintien en séquence est toujours garanti dans les modes orientés connexions.

➤ L'accusé de réception

L'entité destinataire (N) rend compte à l'entité émettrice (N) de la réception correcte ou incorrecte d'une unité de protocole de niveau (N). La technique de l'accusé de réception n'est pas obligatoirement liée au mode connecté. Dans les réseaux locaux, le service dit « LLC3 » implémente un service en mode datagramme avec accusé de réception (l'accusé de réception indique que le message est arrivé et non qu'il a été traité).

➤ La réinitialisation

Les entités communicantes peuvent revenir à un état de référence, la non-perte de données et la non-duplication ne sont pas garanties.

➤ Les données exprès

Les données exprès[4] correspondent à la possibilité d'émettre de petites unités de données. Ces données ne sont pas acheminées plus rapidement par le réseau de transport, cependant elles échappent au contrôle de flux. Ces données sont délivrées, en priorité, par les entités destinataires.

➤ La détection, la correction et la notification d'erreur

Les protocoles (N) peuvent utiliser des fonctions de détection d'erreur et mettre en œuvre des mécanismes de correction (reprise sur erreur). En cas d'échec de la reprise sur erreur, la couche (N) signale à la couche supérieure (N + 1) une erreur non corrigée (notification d'erreur).

➤ La qualité de service

Certaines couches ont la faculté de négocier entre elles, une certaine qualité de service (**QoS**, *Quality of Service*). La qualité de service peut concerner les paramètres suivants :

– délai d'établissement de la connexion ;
– débit ;
– temps de transit, gigue ;
– taux d'erreur résiduelle ;
– coût...

La qualité de service est représentée, dans la demande de connexion, par deux listes, la liste des paramètres relatifs à la qualité demandée et celle relative à la qualité minimale de service acceptable. Si les valeurs minimales ne peuvent être offertes par l'un des sous-réseaux réels traversés ou par l'entité distante, la connexion est refusée.

4. Attention, ISO institue essentiellement un mode connecté. Dans ces conditions, les données émises sur un lien arrivent dans l'ordre, il n'y a pas de données qui peuvent en « doubler » d'autres dans le réseau (données expresses), il s'agit ici de données délivrées à dessein (exprès) et qui seront traitées en priorité.

9.3 ÉTUDE SUCCINCTE DES COUCHES

Nous limiterons cette étude aux fonctionnalités et particularismes essentiels de chacune des couches. Les protocoles et techniques en relation avec ces couches ont déjà fait l'objet d'étude ou le feront lors de l'étude des services qui les mettent en œuvre.

9.3.1 La couche physique

La couche physique (figure 9.17) fournit l'interface avec le support physique sur lequel elle transmet un train de bits en assurant, éventuellement, la transparence de binaire. Elle est chargée de la synchronisation entre les horloges source et destination. La couche physique ne distingue pas le mode connecté du mode sans connexion. Elle prend en charge les transmissions synchrones ou asynchrones en fonctionnement simplex, semi-duplex ou duplex que la liaison soit en mode point à point ou multipoint.

Les services fournis, à la couche liaison, sont :

– l'établissement et la libération de la connexion physique ;
– la transmission série et ou parallèle de « n » bits ;
– l'identification des extrémités de la connexion physique, qui peut être unique (liaison point à point) ou multiple (liaison multipoint) ;
– l'identification du circuit de données, cette identification pouvant être utilisée par les entités réseaux pour identifier un circuit de données (voie logique) ;
– le maintien en séquence des bits émis ;
– l'horloge et la récupération d'horloge (synchronisation) :
– la notification de dérangement.

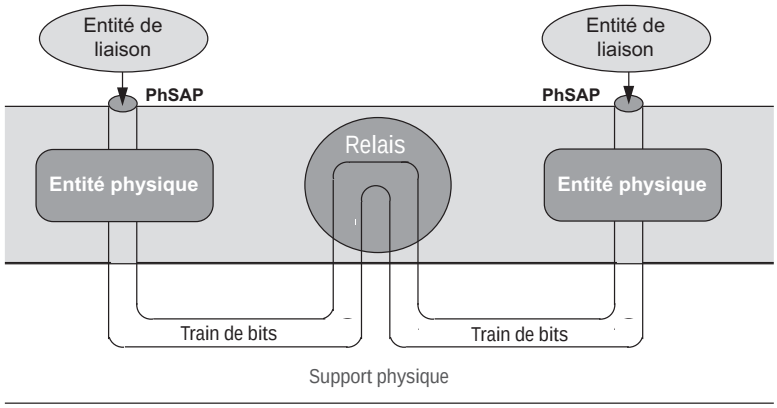


Figure 9.17 La couche physique.

La qualité de service fournie dépend essentiellement des supports utilisés, elle est caractérisée par le débit offert, le débit effectif, le taux d'erreur et la disponibilité.

Les normes couvertes par la couche physique comprennent principalement les normes relatives aux jonctions (V.24, V.35, X.21...) et aux ETCD (Modem, TNR – Terminaison Numérique de Réseau – ...).

© Dunod – La photocopie non autorisée est un délit

9.3.2 La couche liaison de données

La couche liaison de données (figure 9.18) assure le contrôle logique de la liaison et le transfert de données entre entités de réseau sous forme de trame (DL_PDU). La couche liaison de données fournit un service de point à point, dit aussi en **cascade**, et éventuellement un mécanisme de détection et de correction d'erreur.

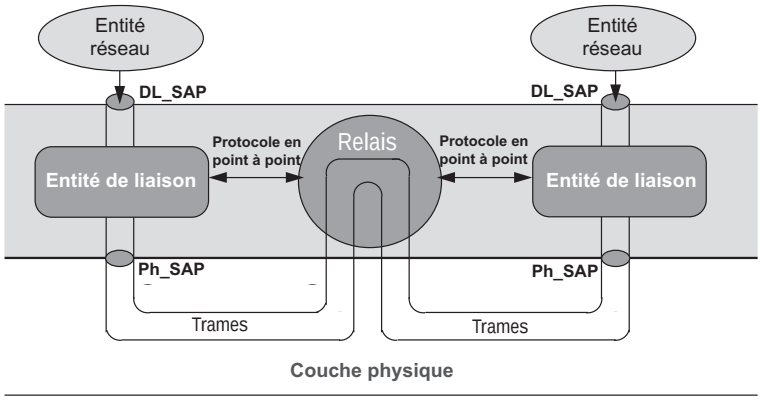


Figure 9.18 La couche liaison de données.

Les services fournis aux entités de réseau, accessibles au SAP dit DLSAP, sont :

– l'établissement, le maintien et la libération de la connexion logique établie entre deux points d'accès au service de liaison de données ;
– éventuellement la fourniture d'identificateur d'extrémité ;
– la délimitation et le transfert des données (trames) en assurant :
  – le maintien en séquence ;
  – la détection et la correction d'erreur ;
  – la notification d'erreur non corrigée ;
  – le contrôle de flux.

La qualité de service fournie s'exprime principalement par le taux d'erreurs résiduelles, ces erreurs pouvant provenir de données altérées, perdues, dupliquées ou du non-respect de l'ordonnancement des trames.

9.3.3 La couche réseau

Structure générale

La couche réseau (figure 9.19) assure un transfert de données entre deux systèmes d'extrémité à travers un ou plusieurs sous-réseaux physiques (systèmes relais). Elle fournit les fonctions de routage et garantit aux entités de transport un service réseau uniforme indépendamment des technologies utilisées dans les sous-réseaux physiques traversés. Deux fonctions essentielles en découlent :

– La localisation des systèmes (adressage).
– L'adaptation de la taille des unités de données (N_PDU) aux capacités des différents sous-réseaux traversés.

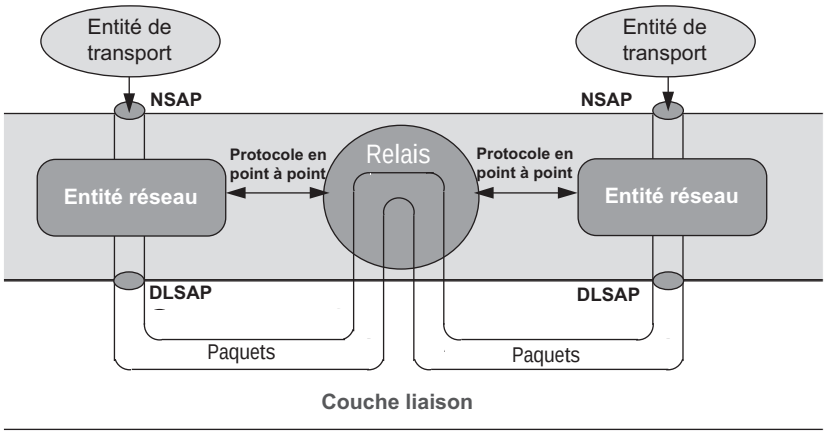


Figure 9.19 La couche réseau.

La localisation du système doit résoudre deux problèmes : l'adressage et l'acheminement (le routage). Le **NSAP** (*Network Service Access Point*) correspond à l'identification, sur les systèmes d'extrémité, de l'accès au service réseau (entités homologues) et non à la localisation du destinataire. Déduit de la NSAP adresse, le **SNPA** (*SubNetwork Point of Attachment*) est couramment appelé adresse du destinataire[5]. Le SNPA identifie le point où le système réel d'extrémité (ou l'unité d'interfonctionnement – relais –) est raccordé au sous-réseau réel (figure 9.20). Le terme de sous-réseau réel désigne le ou les sous-réseaux physiques de transfert, l'emploi du terme réseau est à réserver à la désignation de la couche réseau et des entités réseaux.

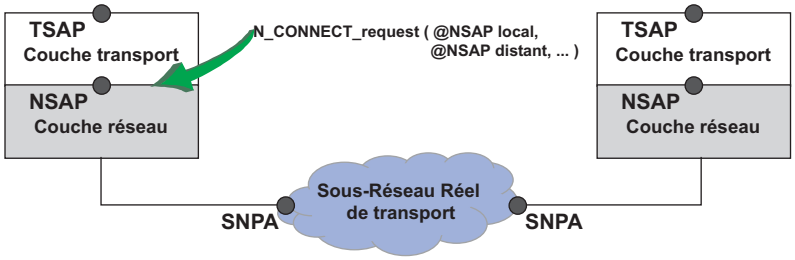


Figure 9.20 L'adressage dans la couche réseau.

L'adresse NSAP (figure 9.21) correspond à un espace d'adressage, appelé **adressage du réseau global**, subdivisé en domaines et contrôlé par une autorité d'adressage (voir chapitre 8, figure 8.28). Étudiée pour s'adapter à tous les types de réseaux, elle est déterminée à partir de la **TSAP** (*Transport Service Access Point*).

La traversée d'un ou plusieurs sous-réseaux nécessite l'adaptation du format et de la taille des données pour être conforme aux possibilités de chaque sous-réseau traversé. Cet impératif explique la complexité réelle de la couche réseau qui doit réaliser :

– éventuellement une conversion d'adresse ;

– l'adaptation de la taille des paquets de données ;

5. Dans la pratique cette distinction n'est pas faite, l'adresse NSAP et le point d'accès au réseau SNPA sont souvent confondus.

© Dunod – La photocopie non autorisée est un délit

– l'adaptation des débits ;
– l'adaptation des modes de fonctionnement, c'est-à-dire le passage du mode connecté au mode non connecté ou inversement.

NSAP		
AFI **Autority and Format Identifier**	**IDI** **Initial Domain Identifier**	**DSP** **Domain Specific Part**
Identifie l'autorité d'adressage, le format et la syntaxe de l'adresse (chiffre de 0 à 99, ex : adressage X.121 AFI= 38).	Identifie le domaine auquel s'applique l'adresse (DSP) c'est, par exemple, le code pays.	Partie spécifique du domaine, c'est l'adresse proprement dite : le **SNPA** (N° Transpac, N° téléphone...).
IDP Initial Domain Part		

Figure 9.21 Structure de l'adressage réseau.

À cet effet, la couche réseau est subdivisée en trois sous-couches qui ne sont pas nécessairement toutes présentes. La couche la plus basse est chargée directement de l'accès physique au sous-réseau réel (**SNACP**, *SubNetwork ACcess Protocol*), la couche la plus haute assure les fonctions réseaux indépendamment du sous-réseau réel utilisé (**SNICP**, *SubNetwork Independant Convergence Protocol*), la couche intermédiaire est chargée d'une éventuelle adaptation (**SNDCP**, *SubNetwork Dependant Convergence Protocol*).

Pour réaliser ses objectifs la couche réseau réalise les fonctions suivantes :

– routage et service relais ;
– connexion de niveau réseau ;
– multiplexage des connexions ;
– segmentation et groupage ;
– détection d'erreur et reprise sur erreur ;
– maintien en séquence ;
– contrôle de flux ;
– transfert de données exprès ;
– réinitialisation.

Exemples d'enchaînement de primitives

➤ Établissement de connexion

L'initiative de l'établissement d'une connexion réseau appartient à la couche transport (figure 9.22). Celle-ci formule sa demande à l'aide de la primitive N_Connect.request dont les paramètres principaux sont les NSAP adresses source et destination et la qualité de service demandée (QoS). N'ayant pas de connexion au niveau liaison, la couche réseau mémorise cette requête et demande à la couche liaison d'établir une connexion de niveau 2 à l'aide de la primitive DL_Connect.request. La demande est traduite par une trame non numérotée SABM[6], la couche 2 distante, à réception de la SABM en réfère à la couche 3 (DL_Connect.ind) ;

6. Pour illustrer le mécanisme d'établissement de la connexion, nous utiliserons, pour le niveau liaison, les unités de données du protocole HDLC, seul protocole étudié jusqu'ici.

celle-ci ayant les ressources suffisantes pour accueillir une nouvelle connexion de niveau liaison accepte et le signifie à la couche 2 par la primitive DL_Connect.response.

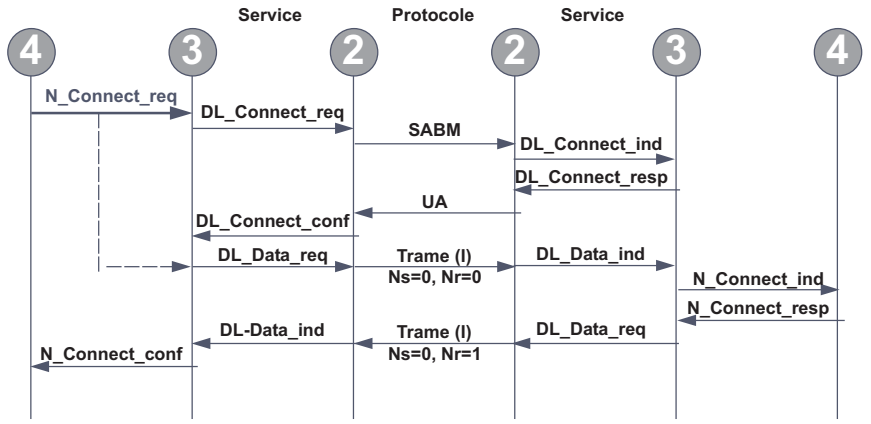


Figure 9.22 Établissement d'une connexion réseau.

La couche acquitte la demande de connexion par la trame (U) UA, à réception de l'UA, la couche 2 locale informe la couche 3 de cette acceptation (DL_Connect.confirm). Disposant d'une connexion de niveau 2, la couche réseau locale peut émettre la demande de connexion réseau en attente (N_Connect.request), cette demande de connexion est transportée dans une unité de données de niveau 2 (DL_Data_.request)[7] traduite en une trame d'information. La couche 2 distante remet cette demande (DL_Data.indication) à la couche 3 distante. De même, celle-ci en réfère à la couche 4 (N_Connect.indication) qui l'autorise à accepter la connexion de niveau 3 (N_Connect.response)... Enfin, la connexion est établie (N_Connect.confirm).

➤ Échange de données

L'échange des données n'appelle aucun commentaire particulier, il est symbolisé figure 9.23.

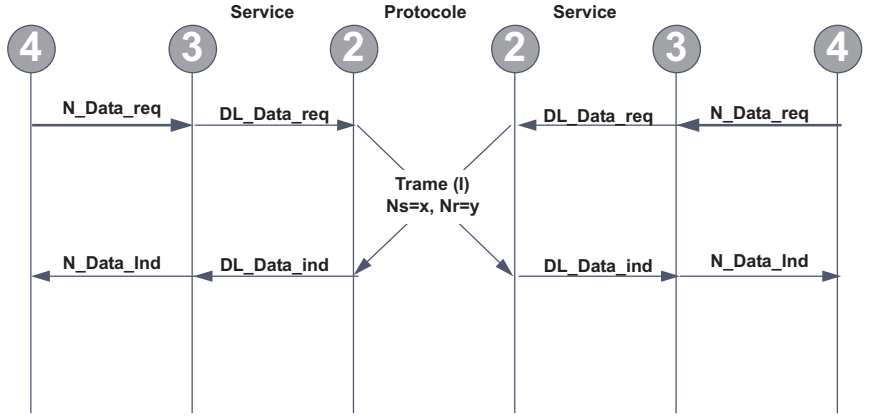


Figure 9.23 Échange de données.

7. Selon le mode utilisé, il existe deux primitives de transfert de données. En mode connecté les primitives se nomment DL_Data_.xxx, et en mode non connecté DL_Unidata.xxx. Pour faciliter la lecture du schéma cette distinction a été volontairement omise.

© Dunod – La photocopie non autorisée est un délit

➤ Rupture de connexion

Le mécanisme de rupture de la connexion de niveau 3 est symétrique à celui de l'établissement. La connexion de niveau 3 est d'abord rompue, puis celle de niveau 2 (figure 9.24).

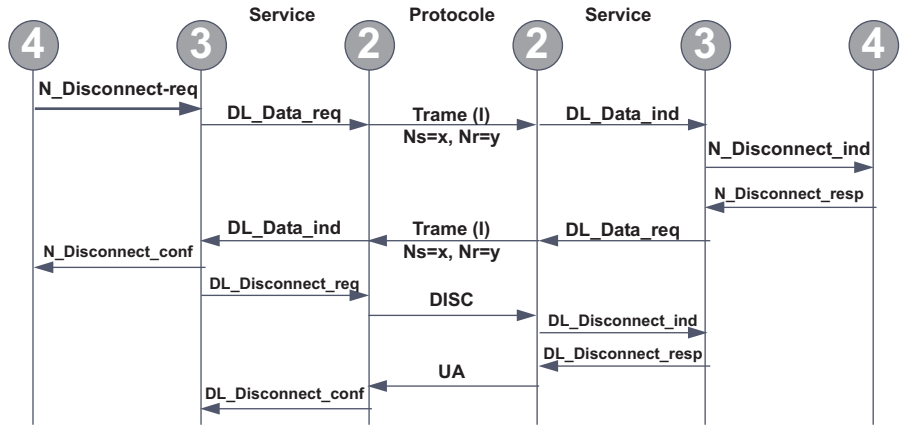


Figure 9.24 Rupture de connexion.

9.3.4 La couche transport

Principes généraux

La couche transport (figure 9.25) garantit aux couches hautes un transfert fiable et transparent des données, en masquant, à celles-ci, les détails d'exécution de ce service. C'est-à-dire qu'elle fournit, aux entités de session, un service de transfert fiable de bout en bout quel que soit le sous-réseau utilisé disponible au SAP TSAP (*Transport Service Access Point*). La couche transport effectue, éventuellement, une remise en séquence des unités de données reçues, si ce service n'est pas garanti par les couches inférieures.

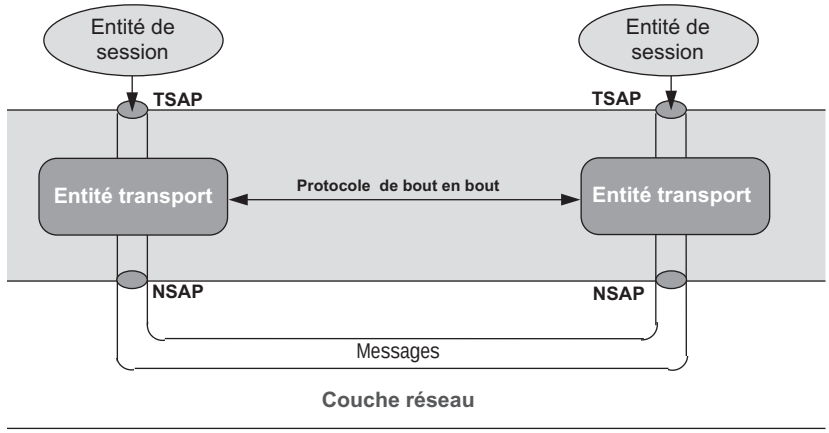


Figure 9.25 La couche transport.

La complexité du protocole de transport est directement liée à la qualité du service réseau utilisé. Les sous-réseaux sont classés en 3 types (A, B et C) en fonction de deux grandeurs (figure 9.26) :

– le taux d'erreurs signalées, les erreurs signalées sont des erreurs détectées par la couche réseau mais non corrigées par celle-ci ;

– le taux d'erreurs résiduelles ou erreurs non signalées.

Type Réseau	Taux d'erreurs résiduelles	Taux d'erreurs signalées	Qualité de service
A	Acceptable	Acceptable	Bonne
B	Acceptable	Inacceptable	Moyenne
C	Inacceptable	Inacceptable	Mauvaise

Figure 9.26 Classification des réseaux selon l'ISO.

Les différentes fonctions de la couche transport visent à améliorer la qualité du service offert par le sous-réseau sous-jacent. Les protocoles de transport sont répartis en 5 classes (classe 0 ou TP0, classe 1 ou TP1 ... classe 4 ou TP4). La classe 0 est la classe de base, elle offre un service minimum, les autres en sont issues par enrichissement successif (figure 9.27).

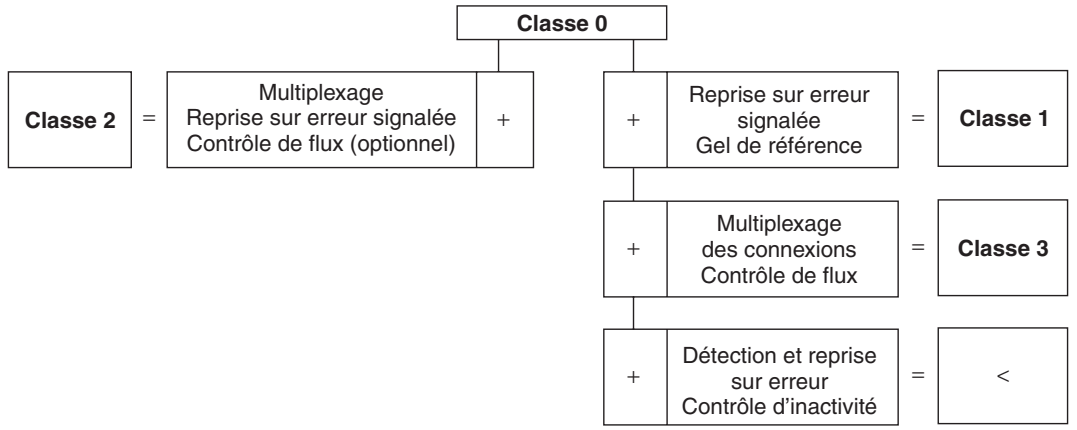


Figure 9.27 Les classes de transport.

La classe de transport, à employer, dépend de la qualité de service offert par les sous-réseaux de transport utilisés. Lors d'une connexion, plusieurs sous-réseaux peuvent être traversés, les hôtes n'ont, en principe, que la connaissance de leur sous-réseau de rattachement. De ce fait, lors de la connexion de transport, la classe de transport employée est l'un des paramètres négociés. La demande de connexion de transport propose une classe préférentielle et, éventuellement, une classe de substitution acceptable. L'entité homologue accepte la classe préférentielle ou celle de substitution, sinon elle propose une classe inférieure de repli. L'appelant peut accepter cette classe de repli ou refuser la connexion.

La figure 9.28 fournit la correspondance entre les différents types de réseau et la classe de transport préconisée.

© Dunod – La photocopie non autorisée est un délit

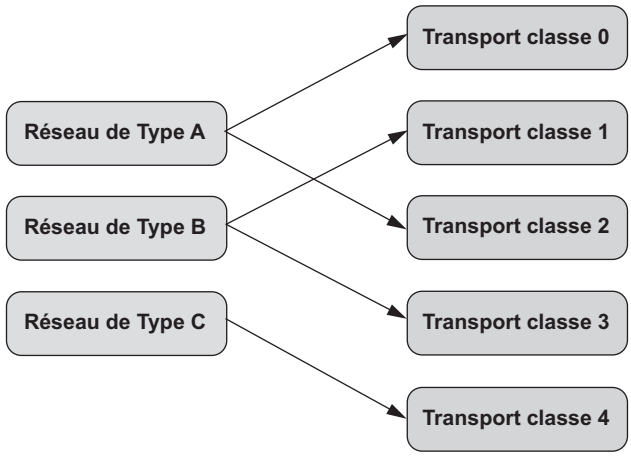


Figure 9.28 Correspondance type réseau et classe transport.

Les mécanismes de la couche transport

Les mécanismes mis en œuvre par les protocoles de transport sont nombreux, quelques-uns sont spécifiques, ils sont détaillés ci-dessous.

– La **résolution de l'adresse de transport**, la localisation de l'entité distante, sur laquelle le système local doit se connecter, est déduite de l'adresse de transport destination (TSAP). Plusieurs cas sont envisageables :
  – le système local connaît la TSAP distante, il émet une demande de connexion à l'adresse de celle-ci ;
  – le système local ne connaît pas la TSAP distante, il peut, dans ce cas, par exemple, se connecter à un service d'annuaire local ou distant qui lui indiquera la TSAP désirée.
– Le **référencement des connexions** de transport, plusieurs connexions de transport peuvent aboutir à une même TSAP. Pour identifier les flux de données de provenances différentes, l'entité de transport attribue à chaque flux un identifiant, sur 2 octets, appelé **référence de transport** (référence source et référence destination). En mode connecté, seule la requête de connexion T_Connect.request transporte, dans la partie option de la T_PDU, l'adresse de transport : TSAP. Dans les autres primitives, la connexion est identifiée par les références source et destination. En mode non connecté (**UD**, *User Datagramme*) et en classe 0 (pas de notion de multiplexage) l'adresse TSAP est toujours présente et le champ référence absent (UD) ou non renseigné (classe 0).
– Le **gel de référence**, lors de la libération d'une connexion, les références de celle-ci ne peuvent être réutilisées, par une nouvelle connexion, pendant un certain temps. Cette technique interdit qu'une nouvelle connexion soit établie sur les mêmes références et reçoive des données, appartenant à la connexion précédente, retardées dans le sous-réseau de transport.
– La **libération implicite ou explicite**, la libération est dite implicite lorsque sa vie est liée à celle de la connexion réseau, elle est réalisée en même temps que celle-ci ; elle est dite explicite quand sa vie est indépendante de celle de la couche réseau.

- La **détection et la correction d'erreur**, (optionnel et en classe 4 uniquement), un total de contrôle est calculé tel que la somme modulo 255 des octets de la T_PDU soit nulle.
- Le **contrôle d'inactivité**, (classe 4 uniquement), une horloge d'inactivité (*timer*) est gérée par l'entité de transport, cette horloge est réinitialisée à chaque réception de T_PDU. À l'échéance du timer, la connexion transport est libérée. Ce mécanisme pallie les libérations de connexion non signalée. Pour éviter, lors de longs silences, une rupture de connexion sur détection d'inactivité, les entités de transport peuvent acquitter les messages (ACK).
- La **segmentation**, lorsqu'une T_SDU est plus grande que la taille des T_PDU autorisée sur le réseau et déterminée à la connexion, celle-ci est segmentée.
- Le **contrôle de flux**, la couche transport utilise un mécanisme dit de contrôle de flux explicite. Le récepteur, en fonction de son état, accorde un crédit à l'émetteur. Le crédit indique, à l'émetteur, le nombre de T_PDU que celui-ci est autorisé à émettre.
- **L'établissement de la connexion en trois temps** (*three ways handshake*), si la demande de connexion est acceptée par le destinataire celui-ci émet, à destination de l'appelant, une T_PDU CC (Connect.confirm). Si le service réseau est un service fiable, la connexion est alors établie et l'échange de données peut débuter (figure 9.29). Si le service réseau est non fiable, un incident quelconque peut survenir et la CC peut, ne jamais, être reçue. Dans ces conditions, l'appelé attend des données qui ne lui parviendront jamais, le système est bloqué (*deadlock*). Pour éviter cette situation, un timer d'inactivité libère la connexion. En classe 4, la connexion ne sera effectivement établie qu'à réception, par l'appelé, d'un accusé de réception de son acceptation (AK), la validation est dite en trois phases (figure 9.29). La T_PDU de demande de connexion (CR) peut transporter un message de 32 octets, ce message peut, par exemple, être un mot de passe.

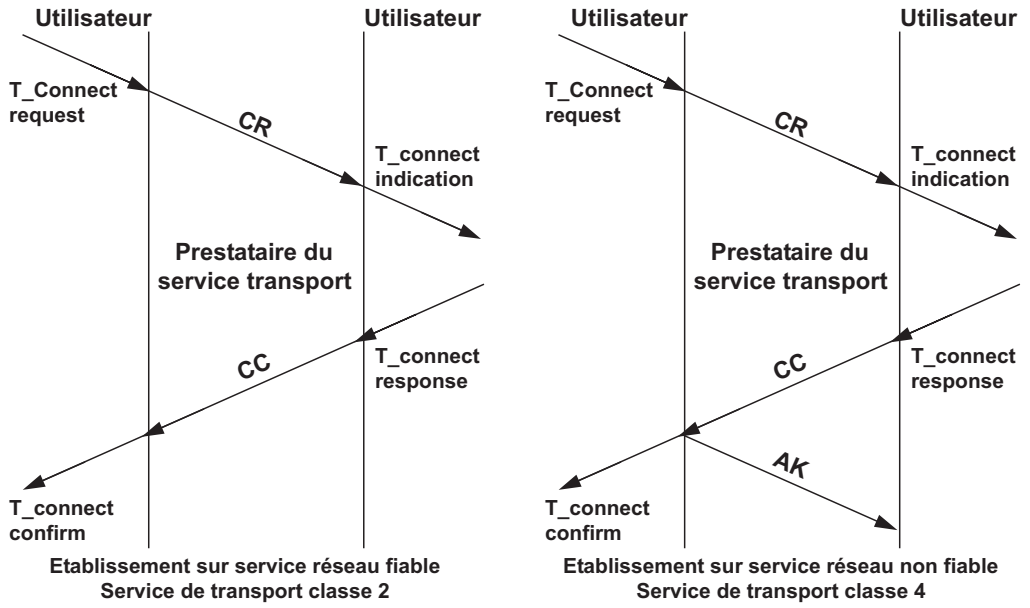


Figure 9.29 Établissement de connexion de transport.

© Dunod – La photocopie non autorisée est un délit

– La **déconnexion**, le mécanisme de déconnexion est identique à celui de la connexion, il peut survenir à n'importe quel moment (déconnexion brutale ou non négociée). De ce fait, des données retardées dans le sous-réseau peuvent être perdues. L'éventuelle perte de données, due à une déconnexion brutale est, en fait, traitée par la couche session.

Mécanismes mis en œuvre par les protocoles de transport	**Classes**				
	0	**1**	**2**	**3**	**4**
Affectation à une connexion réseau	•	•	•	•	•
Établissement de connexion	•	•	•	•	•
Refus de connexion	•	•	•	•	•
Traitement des erreurs de protocole	•	•	•	•	•
Libération sur erreur	•		•		
Resynchronisation		•		•	•
Multiplexage et démultiplexage			•	•	•
Contrôle de flux (A avec, S sans) **de bout en bout**	**S**	S	**AS**	**A**	A
Libération normale (I implicite, E explicite)	**I**	E	**E**	**E**	E
Numérotation des TPDU (S sans, N normale, E étendue)	**S**	N	**NE**	**NE**	NE
Gel de référence		•		•	•
Segmentation et réassemblage	•	•	•	•	•
Concaténation et séparation		•	•	•	•
Remise en séquence					•
Total de contrôle optionnel (**détection d'erreur de bout en bout**)					•
Retransmission après temporisation					•
Éclatement et recombinaison					•
Détection d'inactivité					•

Figure 9.30 Synthèse des différents mécanismes de la couche transport.

La figure 9.30 rappelle les principales fonctions mises en œuvre par les différentes classes de transport.

Protocole de transport sans connexion

Le protocole de transport, en mode connecté, est lourd à mettre en œuvre, un additif à la norme (ISO 7498) spécifie un protocole en mode non connecté. Les fonctions assurées sont réduites : mise en correspondance de l'adresse de transport et de l'adresse réseau (NSAP), délimitation des blocs de données (T_PDU), détection d'erreur et choix du service réseau le mieux adapté.

Si le service transport, en mode non connecté, est associé à un service réseau, aussi en mode non connecté, aucune garantie de remise ni de séquencement n'est assurée à la couche session. Les unités de données ne sont pas acquittées, un total de contrôle optionnel peut être utilisé.

9.3.5 La couche session

La couche session est l'interface entre le processus d'application et le service de transfert de données (connexion de transport). Elle assure au processus d'application[8] les moyens de contrôler le dialogue en organisant celui-ci et en autorisant les reprises (resynchronisation).

La gestion du dialogue et la synchronisation sont assurées par l'intermédiaire de 4 jetons :

– le jeton de données qui contrôle l'accès au transfert de données lors d'un échange à l'alternat ;
– le jeton de terminaison qui autorise le détenteur à demander une libération normale de la connexion de session ;
– le jeton de synchronisation mineure (mi) qui permet la pose d'un point de synchronisation mineure ;
– le jeton de synchronisation majeure (MA) et d'activité qui autorise la pose d'un point de synchronisation majeure ou qui délimite le début et la fin d'une activité.

Un jeton est disponible ou indisponible. S'il est indisponible, aucun utilisateur ne peut bénéficier des services qui lui sont associés. L'entité qui ne possède pas le jeton peut le demander (*Please Token*), celle qui le possède peut le lui concéder (*Give Token*) ou ignorer la demande. Dans le cadre d'un dialogue en full duplex, aucune entité n'a l'usage exclusif du jeton.

La structuration du dialogue est garantie par la pose de points de synchronisation. Un point de synchronisation permet d'identifier des instants significatifs de l'échange. Il est posé sous la responsabilité du processus d'application (services reflétés), son identification est à la charge de la couche session.

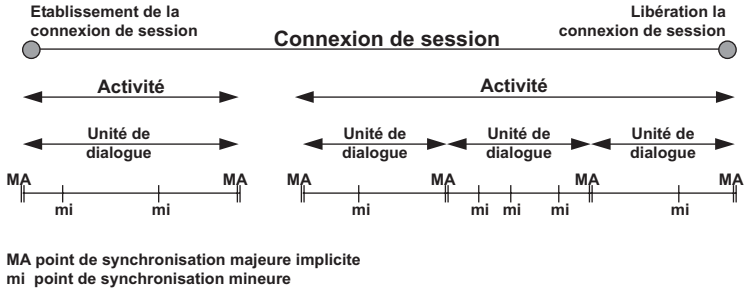


Figure 9.31 Activité, dialogue, points de synchronisation.

Une connexion de session est découpée en activités (figure 9.31). Une activité correspond à un transfert autonome de données, par exemple le transfert d'un fichier. Une session peut comporter une ou plusieurs activités, de même une activité peut être couverte par plusieurs sessions. Une activité est découpée en unités de dialogue, elles-mêmes séparées par des points de synchronisation majeure. La pose d'un point de synchronisation majeure suppose que toutes les données précédemment transmises sont correctes. Lorsqu'une activité est interrompue ou en cas d'erreur de transmission, il est possible de reprendre le transfert à partir d'un point

8. Les services de la couche session sont dits réfléchis ; la couche présentation est transparente en ce qui concerne l'organisation du dialogue, celui-ci est directement contrôlé par la couche application (voir couche application section 9.4.7).

© Dunod – La photocopie non autorisée est un délit

de synchronisation (resynchronisation). À l'intérieur d'une unité de dialogue, il est toujours possible de revenir et de resynchroniser le dialogue sur un point de synchronisation mineure appartenant à l'unité de dialogue en cours et ce, jusqu'au dernier point de synchronisation majeure posé. Le début et la fin d'une activité correspondent à des points de synchronisation majeure implicite.

9.3.6 La couche présentation

Fonctionnalités

La couche présentation (figure 9.32) est la première couche non impliquée dans les mécanismes de transfert d'information. Son rôle essentiel consiste à garantir la signification des données transférées, indépendamment de la représentation interne de celles-ci, du codage utilisé (ASCII, EBCDIC...), de la longueur des mots machines (32, 64 bits...), de la représentation des valeurs négatives (complément à 1 ou à 2) dans les hôtes communicants.

La couche présentation garantit à la couche application :

– l'accès aux services de la couche session, la plupart des primitives de service de présentation ne font que traverser la couche présentation, elles ont une correspondance directe avec les primitives de service de la couche session (services réfléchis) ; ainsi, par exemple, l'invocation, par la couche application, de la primitive de service P_TOKEN_PLEASE.request se limite à appeler la primitive S_TOKEN_PLEASE.request ;
– les services de cryptographie et de compression de données ;
– la négociation d'une syntaxe de transfert (contexte de présentation) lors de l'établissement de la connexion de présentation.

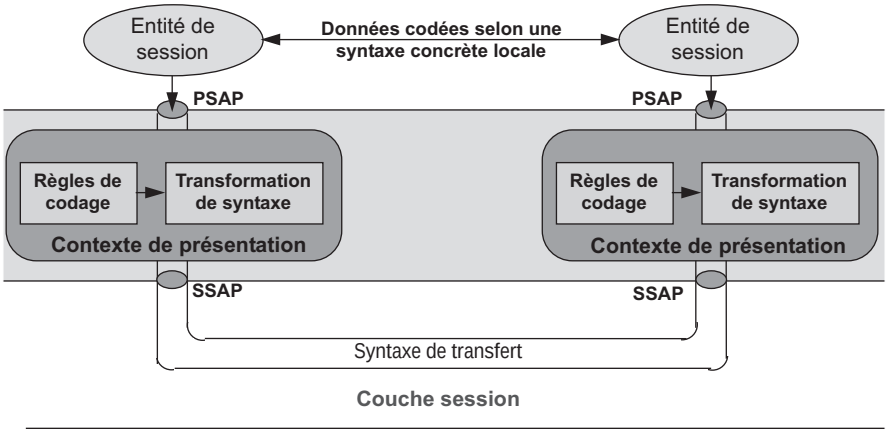


Figure 9.32 La couche présentation.

Notions de syntaxe concrète, abstraite et de transfert

Les données manipulées par l'application sont formatées selon une certaine structure dite **structure de données** (« record » ou enregistrement). La signification des données dépend

de l'application utilisateur, la valeur qui leur est assignée est liée à la représentation interne des nombres dans la machine. Ces données sont codées selon une syntaxe concrète locale directement fonction du contexte (processus applicatif utilisateur, machine cible...). Afin de garantir l'interprétation identique des données entre entités d'application distantes, celles-ci négocient une représentation commune des données, c'est la **syntaxe de transfert**.

La syntaxe de transfert (figure 9.33) est obtenue par transformation (codage) de la syntaxe concrète locale à l'aide de règles de codage, les données étant présentées selon une syntaxe indépendante du contexte, c'est la syntaxe abstraite[9].

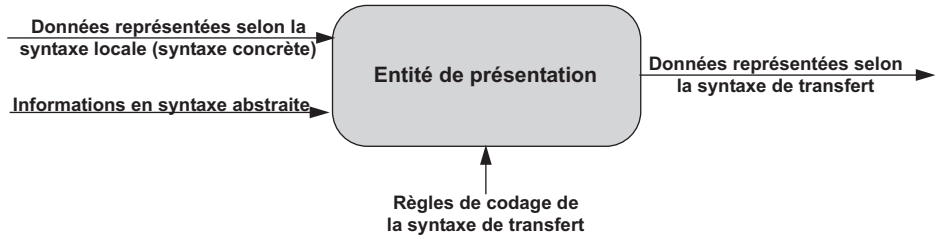

Données représentées selon la syntaxe locale (syntaxe concrète)
Informations en syntaxe abstraite
Entité de présentation
Données représentées selon la syntaxe de transfert
Règles de codage de la syntaxe de transfert

Figure 9.33 Principe d'élaboration d'une syntaxe de transfert.

L'ISO a défini une notation pour spécifier une syntaxe abstraite des données : la notation de syntaxe abstraite N° 1 (**ASN 1** ou ISO 8824 *Abstract Syntax Notation 1*). ASN1 fournit :

– une méthode pour décrire (syntaxe) les données échangées indépendamment des processeurs et systèmes d'exploitation ;

– un ensemble de types de données de base (types simples ou primitifs) pouvant être employés pour en construire d'autres (types construits) ;

– un ensemble de règles de construction de ces types et les opérateurs associés.

La figure 9.34 donne en exemple quelques types de données.

ID	Types Primitifs	Signification
2	INTEGER	Entier de taille arbitraire, utilisable pour définir des types énumérés.
1	BOOLEAN	Valeur alternative : False ou True.
3	BIT STRING	Liste de 0 ou de bits en binaire pur '00011001'B ou en hexadécimal '3D'H.
4	OCTET STRING	Liste d'octets
5	NULL	Définit un objet sans type, n'est pas transmis.
6	OBJET IDENTIFIER	Permet d'identifier, par une chaîne de caractères, un objet dans un protocole.
	Types Constructeurs	
16	SEQUENCE	Autorise la construction de types complexes (similaire au record du langage Pascal).
16	SEQUENCE OF	Définit un tableau de valeurs d'un même type.
17	SET	Représente un ensemble non ordonné d'objets de types quelconques.
17	SET OF	Ensemble d'objets de même type.

Figure 9.34 Exemple de types de données.

9. On parle également de « langue pivot ».

© Dunod – La photocopie non autorisée est un délit

Exemple :

La structure représentative de l'identité d'un individu pourrait être codée :

```
Individu : :=     SEQUENCE {
                          nom              OCTET STRING, – 20
                          prenom           OCTET STRING, –20
                          age              INTEGER,
                          sexemasculin     BOOLEAN
                          }
```

L'expression –20 est un commentaire qui indique la longueur de la chaîne.

À chaque type est associée une étiquette (ID) qui permet d'identifier la nature de la donnée transmise. La chaîne de caractères « BONJOUR » (ID 4, voir figure 9.36) sera transmise selon le codage de la figure 9.35, ce qui correspond à la syntaxe de transfert.

Type	Longueur	Valeur
4	7	BONJOUR
ou en hexadécimal		
4	7	42 4F 78 74 4F 85 82

Type (4)	Chaîne de caractères	est représentative de la syntaxe abstraite ;
Valeur	BONJOUR	est la valeur codée en ASCII, c'est la syntaxe concrète ;
Codage	04 07 42 4F 78 74 4F 85 82	est la valeur transmise, c'est la syntaxe de transfert.

Figure 9.35 Exemple de syntaxes.

9.3.7 La couche application

Structure générale

La couche application est la dernière couche et la plus abstraite du modèle OSI, ses utilisateurs ne sont pas des entités d'une couche supérieure mais l'application utilisateur proprement dite (**AP**, *Application Process* ou **UAP** *User Application Process*). Elle a pour objet de fournir tous les mécanismes nécessaires au fonctionnement des programmes utilisateurs situés sur des machines distinctes et interconnectées.

Ces mécanismes sont réunis en ensembles homogènes de fonctions rendant un service défini (**ASE**, *Application Service Element*). Un ASE est un service normalisé communiquant avec l'ASE homologue distant par un protocole normalisé[10]. Les différents services offerts par les ASE sont accessibles à l'applicatif utilisateur via une interface (**UE**, *User Element*). Cette interface se présente comme un ensemble de librairies de procédures et de fonctions constituant des appels normalisés aux ASE.

Attention, un processus d'application constitue un tout homogène, la séparation entre l'application utilisateur et la couche application n'est que conceptuelle. Dans ces conditions, la structure générale de la couche application peut être représentée comme l'indique la figure 9.36.

10. Ce qui a fait dire à certains que la couche application était constituée d'un ensemble de sous-couches, cette vision est erronée.

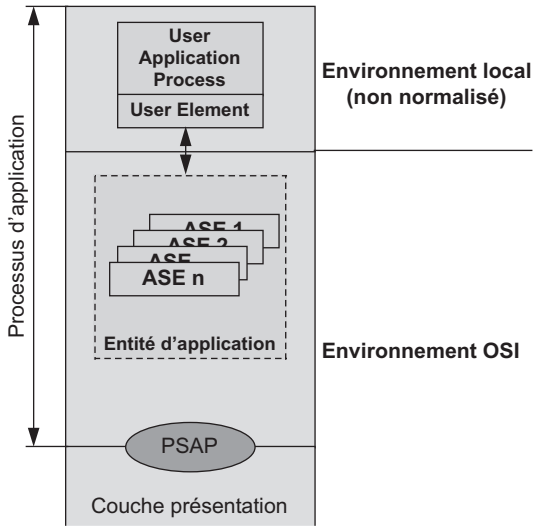


Figure 9.36 Structure générale de la couche application.

Les ASE

Les ASE peuvent offrir des services banalisés couramment utilisés par toutes les applications, ce sont les **ASE de base**. Lorsque les ASE sont dédiés à des tâches spécifiques ils sont dits **ASE fonctionnels**[11].

➤ Les ASE de base

ACSE (*Association Control Service Element*), ISO 8649 et 8650 CCITT X.217 et X.227, cet ASE appartenant à toute association gère la connexion (l'association), il assure l'établissement, le maintien, la libération ou l'abandon d'une association.

CCRSE (*Commitment, Concurency and Recovery Service Element*, engagement, concurrence et reprise), ISO 9804 et 9805, garantit l'intégrité des transactions, il est utilisé chaque fois que les applications exigent un certain niveau de sécurité, par exemple l'intégrité d'un système de bases de données réparties. CCRSE assure la cohérence globale des transactions en définissant une action atomique. Une action atomique comprend un nombre de tâches qui doivent toutes être réalisées ou pas du tout. En cas de défaillance, le système est rétabli dans son état d'origine. Il permet la mise en place des éléments protocolaires associés au protocole de validation à 2 phases utilisé pour rendre une opération atomique.

RTSE (*Reliable Transfer Service Element*), ISO 9066, CCITT X.218 et X.228, initialement prévu pour le transfert de documents dans la messagerie X.400, RTSE est devenu un service de base. Il offre un service fiable de transport de données en assurant les reprises en cas de défaillance d'un des systèmes d'extrémité.

11. La distinction ASE fonctionnels et ASE de base est préférable à celle d'éléments de service d'application spécifique (SASE, *Specific Application Service Element*) pour les ASE fonctionnels et d'éléments de service d'application commun (CASE, *Common Application Service Element*) pour les ASE de base.

© Dunod – La photocopie non autorisée est un délit

ROSE (*Remote Operation Service Element*)**,** ISO 9072, CCITT X.219 et X.229, comprend un ensemble de fonctions supportant les opérations interactives. ROSE est notamment utilisé dans le modèle client/serveur.

➤ Les principaux ASE fonctionnels

MHS (*Message Handling System***,** système de messagerie), ISO 10021, CCITT X.400/MOTIS, implémente un service de messagerie en mode non connecté. En cas d'absence du destinataire, le message est délivré dans sa boîte à lettres. X.400 offre les services de création, envoi, réception et stockage de messages.

DS (*Directory Service*), ISO 9594, CCITT X.500, offre un service d'annuaire, c'est une base de données permettant la localisation géographique (adresse) des équipements adressables connectés au réseau. La norme prévoit un seul annuaire mondial, en fait, il s'agit de réaliser un ensemble d'annuaires locaux coopérants. Les éléments sont adressés selon une organisation hiérarchique ou en arbre (**DIT**, *Directory Information Tree*). X.500 assure la correspondance entre un nom mnémonique et une adresse physique.

FTAM (*File Transfer, Access and Management*), ISO 8571, assure les opérations d'accès, de transfert et de gestion de fichiers distants. FTAM travaille sur des fichiers virtuels ou documents, c'est le système d'exploitation qui manipule les fichiers physiques. Trois types génériques de fichiers sont décrits dans FTAM :

– Les fichiers non structurés, dans ce type de fichiers, les applications ne connaissent pas la structure de ceux-ci, seules les opérations de lecture et d'écriture portant sur l'intégralité du fichier sont admises.

– Les fichiers structurés, constitués d'une suite d'enregistrements éventuellement associés à une clé. Il est possible d'accéder à un enregistrement spécifique, séquentiellement ou à l'aide de la clé associée. Toutes les opérations sur les fichiers sont autorisées : lecture, écriture, modification suppression ou ajout d'enregistrement.

– Les fichiers hiérarchisés, modèle plus général, ce type de fichier peut être représenté par un arbre, à chaque nœud est associée une clé.

DTP (*Distributed Transaction Processing*), ISO 10026, cet ASE est spécialement dédié à la gestion de transactions s'exécutant sur des terminaux répartis. DTP utilise la notion de transaction atomique afin de garantir l'intégrité des données (fichiers cohérents).

VT (*Virtual Terminal*), ISO 9040 et 9041, définit un terminal virtuel (nombre de lignes, nombre de caractères par ligne, attributs de caractères, fontes...). Il assure la correspondance entre les caractéristiques du terminal virtuel et le terminal du système physique réel. VT gère les différents types de terminaux :

– terminal en mode défilement ou rouleau ;

– terminal en mode page ;

– terminal en mode masque d'écran et données ;

– terminal graphique simple ou multifenêtre.

ODA (*Office Document Architecture*), ISO 8613, CCITT T.400, normalise une architecture de documents, ODA concerne le traitement de textes. ODA spécifie une structure générale de document comprenant :

– Le profil du document, ensemble d'informations caractérisant un document (titre, objet, date de création, dernière mise à jour, auteur...).
– La structure logique, structure le document en chapitres, sections, paragraphes, table des matières, références...
– La structure physique, décrit le document pour en assurer la reconstitution (fontes de caractères, nombre de colonnes...), elle est en correspondance directe avec la structure logique.

ODA reconnaît les textes en mode caractères (T.416), les dessins en mode points (T.417), les dessins en mode vectorisé (T.418). Le format d'échange des documents est défini par *ODIF (Office Document Interchange Format*).

JTM (*Job Transfer and Manipulation*) a pour objet la manipulation de documents (ensemble de fichiers dans le monde ISO). JTM distingue l'initiateur, processus ou utilisateur qui soumet le travail, la source ou système de gestion de fichiers, le puits ou destinataire des fichiers et l'exécuteur, la (ou les) machine (s) qui effectue(nt) les travaux.

RDA (*Remote Databade Access*) définit un modèle d'accès aux bases de données en proposant un modèle général : le modèle client/serveur.

9.3.8 Devenir du modèle OSI

Au début des années 1980, le modèle OSI a suscité de grands espoirs. La plupart des constructeurs avaient entrepris des travaux de migration de leur architecture propriétaire vers l'architecture OSI. Mais devant la lenteur des travaux de normalisation, la complexité des solutions adoptées et la non-conformité aux exigences des nouvelles applications, le modèle de référence n'a jamais fait l'objet de véritables implémentations complètes. Cependant, OSI en structurant les fonctions décrit tous les concepts et les mécanismes nécessaires au développement d'une architecture de communication, il demeure et restera une référence pour les autres architectures et un parfait modèle pédagogique.

Le modèle de référence et le temps réel

➤ Définitions

On a l'habitude de désigner par temps réel les applications où l'opérateur est en relation directe avec le système dont il attend une réponse. Ces applications doivent être appelées : applications interactives (réservation, consultation de bases de données...). Dans ce type d'application, il n'y a pas de contrainte réelle de temps. Il faut réserver la dénomination « temps réel » aux systèmes qui, non seulement, sont soumis à des contraintes temporelles sévères mais où les événements doivent être datés. Dans ces systèmes, l'information a une durée de vie limitée. Même, si l'information est syntaxiquement exacte sa signification peut être erronée ; c'est, par exemple, le cas de la transmission d'une information horaire, si celle-ci est précise au centième de seconde, la durée de validité, de l'information transmise, n'excède pas le centième de seconde. Il ne faut pas confondre non plus temps réel et transfert isochrone, un transfert isochrone est un transfert dont la cadence de réception des messages ne souffre pas de décalage entre eux, le temps de transmission pouvant être indifférent.

Ces applications se rencontrent surtout dans les processus industriels (gestion d'un mobile, acquisition de données d'état...) et dans les systèmes d'arme (conduite de tir).

© Dunod – La photocopie non autorisée est un délit

➤ L'incompatibilité temps réel et modèle OSI

Le modèle OSI définit des niveaux fonctionnels qui fournissent chacun un service spécifique. OSI résout les problèmes d'interconnexion d'équipements hétérogènes, mais ne prend pas en compte le critère temps.

Dans la pratique, le traitement des données correspond à une suite de procédures dont l'enchaînement peut être matérialisé, à la frontière de chaque couche, par une file d'attente. Cette approche est incompatible avec la prise en compte des contraintes temporelles imposées par le temps réel. Cette remarque est valable pour toutes les architectures en couches. La prise en compte des applications dites temps réel impose l'implémentation de mécanisme particulier de contrôle des échanges.

Le modèle de référence et les hauts débits

La structure complexe du modèle de référence et les traitements qu'elle induit ne permettent pas aux protocoles conformes au modèle OSI d'évoluer vers les hauts débits. Les principaux handicaps proviennent essentiellement de la redondance des traitements d'une couche à l'autre, des mécanismes de reprises sur erreur et de la signalisation dans la bande qui conduit à des en-têtes variables (PCI) dont l'analyse pénalise les performances des différents relais.

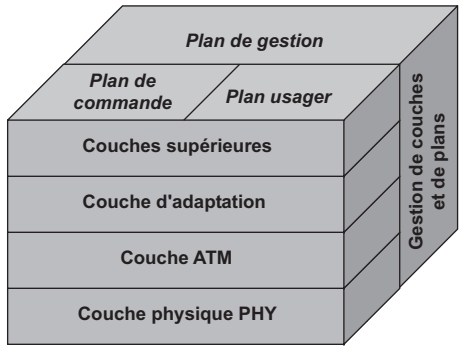


Figure 9.37 Le modèle de l'UIT.

C'est lors de la description de l'architecture du **RNIS-BE** (Réseau Numérique à Intégration de Services Bande Étroite ou **ISDN**, *Integrated Service Data Network*) que le modèle de référence a montré ses insuffisances. En effet, ce dernier organise et contrôle l'interfonctionnement d'applications informatiques alors que le RNIS ne se préoccupe que du transport de bout en bout de données multimédia. Tandis que le modèle OSI suppose que les données de gestion et de contrôle sont transportées de la même façon que les données usagers (signalisation dans la bande), le RNIS transporte celles-ci de manière indépendante (signalisation par canal sémaphore).

Le modèle de l'IUT, défini pour RNIS-BE, a été repris pour le RNIS-LB (RNIS Large Bande). Ce modèle (recommandation I.321) comporte quatre couches dites couches de communication (figure 9.37) regroupant trois plans indépendants les uns des autres : le plan usager, le plan de commande, et le plan de gestion.

Le plan usager (*User Plane*) a en charge le transfert des informations utilisateurs, le contrôle d'erreur et le contrôle de flux. Le plan de commande (*Control Plane*) comporte tous les

mécanismes de signalisation nécessaires à l'établissement, au maintien et à la libération de la connexion. Le plan de gestion (*Management Plan*e) assure la gestion des performances, la localisation des défaillances (*fault*), la détection des pannes et la mise en œuvre des mécanismes de protection du système (reconfiguration...), le plan de gestion utilise un flux de cellules spécifiques (**OAM cells**, *Operation And Maintenance cells*). Contrairement aux données de gestion qui utilisent un canal spécifique (canal sémaphore), les cellules OAM sont multiplexées avec toutes les autres données transportées par le système.

Une autre particularité de ce modèle est d'avoir introduit une couche d'adaptation (**AAL**, *Adaptation ATM Layer*), interface entre le transport de données (couche ATM) et les applications. La couche AAL met en œuvre des mécanismes spécifiques à chaque type de données transportées autorisant ainsi le transport banalisé des données.

9.4 LES ARCHITECTURES CONSTRUCTEURS

9.4.1 Architecture physique d'un système de téléinformatique

Les besoins croissants en terminaux connectés ont conduit les constructeurs à définir, bien avant l'avènement du modèle OSI, une architecture physique type autour de leur calculateur (*mainframe*, hôte ou host). Afin, de décharger l'hôte de la gestion des télécommunications, un ordinateur périphérique ou frontal de communication a pris en charge la gestion générale du réseau et des terminaux. De manière similaire et afin d'optimiser l'utilisation des liens, des équipements de concentration (contrôleur de grappe de terminaux) ont été utilisés (figure 9.38).

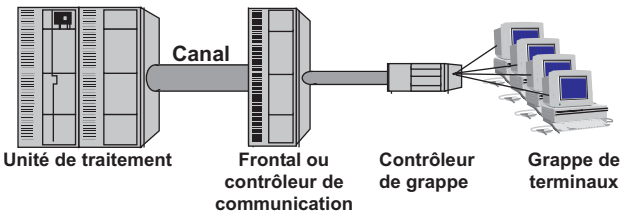


Figure 9.38 Structure d'un système informatique.

Le contrôleur de communication (frontal) gère l'ensemble des moyens logiciels et physiques (terminaux isolés, grappes de terminaux via des concentrateurs, liaisons privées ou publiques). La figure 9.38 illustre les réseaux propriétaires autour d'un *mainframe*.

9.4.2 Origine des architectures constructeurs

La normalisation succède à un état de fait, aussi le modèle OSI n'est apparu que parce que l'interconnexion d'équipements hétérogènes était devenue complexe par la diversité des problèmes à résoudre. En effet, les constructeurs n'avaient pas attendu les travaux de l'ISO pour définir l'environnement d'interconnexion de leurs équipements. Ces environnements (ou architectures propriétaires) sont nés dans les années soixante-dix (IBM avec SNA en 1975, BULL avec DSA en 1979, DEC avec DNA).

La figure 9.39 représente les principales architectures propriétaires. Elles ont en commun une structuration en couches mais les approches peuvent être totalement différentes. Par

© Dunod – La photocopie non autorisée est un délit

exemple, OSI est orienté service alors que SNA est orienté fonction. Globalement, tous les services à offrir sont fournis dans les architectures propriétaires mais ils ne sont pas obligatoirement localisés dans une couche en correspondance directe avec le modèle OSI et peuvent, éventuellement, être éclatés en plusieurs couches ; c'est, par exemple, le cas de la session OSI qui recouvre approximativement la couche contrôle de flux et contrôle de transmission de l'architecture SNA.

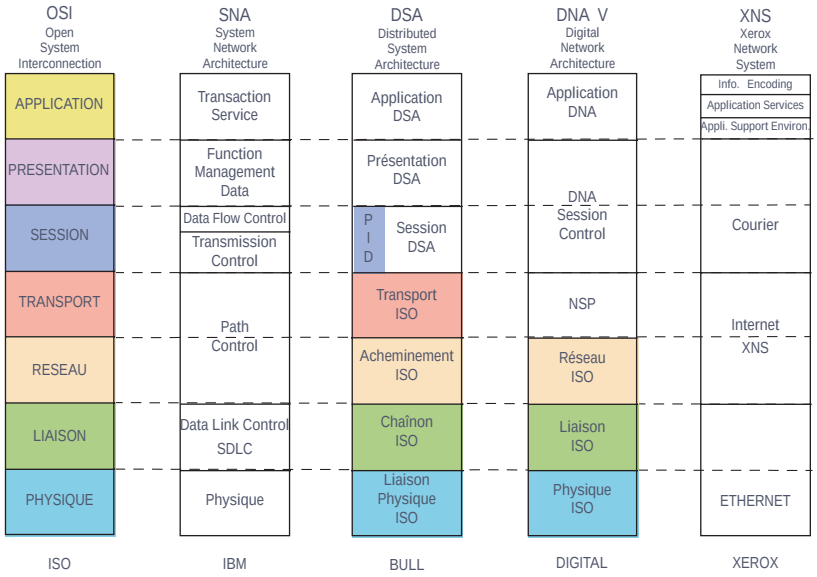


Figure 9.39 Les architectures propriétaires et OSI.

Une architecture propriétaire s'applique à un réseau physique spécifique et formalise les concepts fondamentaux qui ont conduit les constructeurs à tel ou tel choix. Pour illustrer ces propos et compte tenu que les architectures propriétaires survivront encore un certain temps, le paragraphe suivant se propose d'examiner rapidement les deux architectures les plus répandues en France, celle d'IBM et celle de BULL.

9.4.3 SNA (System Network Architecture) d'IBM

Concepts de base

Afin de garantir l'évolutivité de son système, indépendamment des évolutions des matériels, les constituants du réseau ne sont vus, dans SNA, que par leur représentation logique. Le réseau logique SNA est constitué d'unités réseaux adressables (**NAU**, *Network Adressable Unit*). Les NAU sont connus du réseau par un nom et une adresse réseau, il existe trois types de NAU :

– Les **SSCP** (*System Services Control Protocol*) ou centres directeurs : un SSCP est l'unité de gestion d'un domaine (matériellement l'hôte). La fonction SSCP est implémentée dans la méthode d'accès VTAM et assure le contrôle des ressources du réseau, mise en route, activation désactivation, collecte des messages d'erreur, établissement et clôture des sessions.

– Les **PU** (*Physical Unit*) : l'unité physique est un programme qui gère les ressources physiques d'un matériel à la demande du SSCP. Elle assure l'activation, la désactivation et le

test des lignes, le recouvrement des erreurs et la collecte des données statistiques sur le fonctionnement du nœud. Chaque nœud SNA est une PU, il existe autant de type de PU que de types de nœuds. Il n'existe pas de PU de type 3. La figure 9.40 situe chaque PU dans l'architecture SNA et indique les principales fonctions remplies par chacune d'elle.

– Les **LU** (*Logical Unit*) sont la représentation de l'usager (EU ou *End User*) ce sont des applications ou des terminaux. Une LU constitue un ensemble de fonctions qui fournit à l'usager un point d'accès au réseau. On distingue deux types de LU, les LU primaires (application ou programme) et les LU secondaires (terminal). On classe les LU selon le mode de communication qu'elles établissent entre elles (session). La figure 9.41 cite les différentes LU de l'architecture SNA.

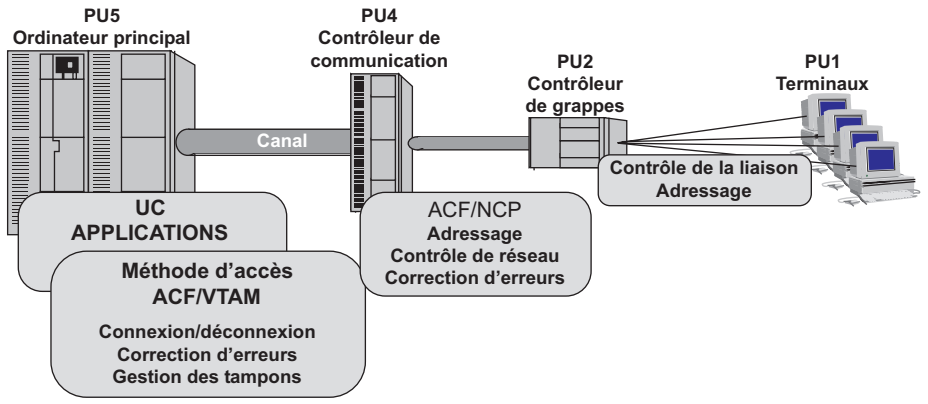


Figure 9.40 Les différents types d'unités physiques de SNA[13].

Classe de LU	Type de session LU-LU
LU 0	Support de protocoles particuliers pour les couches supérieures.
LU 1	Processus d'application en session avec un ou plusieurs terminaux en mode batch ou interactif.
LU 2	Processus d'application en session avec une console de visualisation.
LU 3	Processus d'application en session avec un terminal de type imprimante.
LU 4	Processus d'application en session avec un terminal du type station de travail ou session de terminal à terminal.
LU 6-1	Session de programme à programme dans un traitement distribué (sessions parallèles)
LU 6-2	Session de programme à programme en mode peer to peer (APPC) Session entre PU5, entre PU5 et PU2-1 ou entre deux nœuds de type 2-1.
LU 7	Processus d'application (programme interactif) en session avec une station de travail.

Figure 9.41 Les classes d'unités logiques de SNA.

Le modèle SNA

Dans SNA, deux usagers (**EU**) échangent des unités de données (**RU**, *Request/Response Unit*) de manière similaire à celle du modèle de référence, des informations de gestion (figure 9.42) sont ajoutées en préfixe (*Header*) et en suffixe (*Trailer*) afin de :

© Dunod – La photocopie non autorisée est un délit

– définir le format des messages ;
– identifier les protocoles utilisés ;
– assurer l'acheminement correct des RU ;
– fournir l'identification des usagers origine et destination ;
– délimiter les trames.

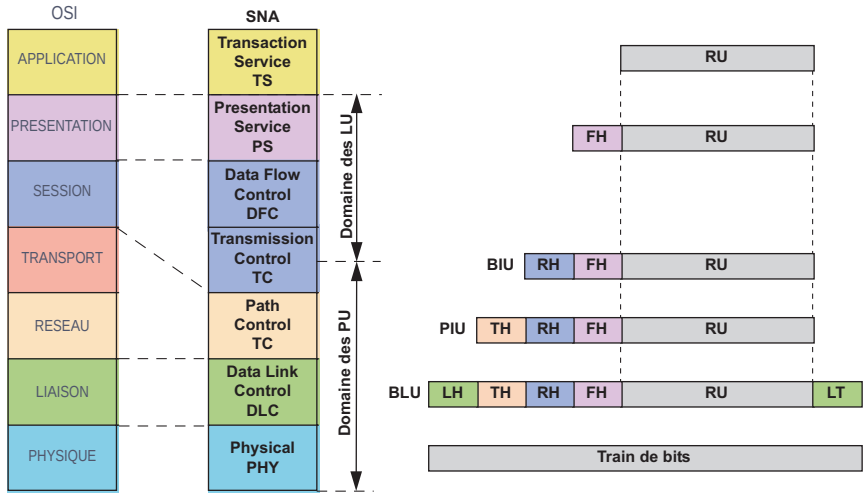


Figure 9.42 Les unités de données dans SNA.

Contrairement à OSI, toutes les couches n'ajoutent pas directement d'informations de gestion aux unités de données. Cependant, dans ce cas, elles fournissent les éléments nécessaires à la couche inférieure pour que celle-ci les mette dans son propre en-tête.

L'utilisateur final (EU) accède via les services de transaction (**TS**) aux services de présentation (**PS**) constitués d'un gestionnaire de service et d'un interpréteur gestionnaire de données. L'en-tête (**FMH**, *Function Management Header*) contient les informations relatives au type, au code, au cryptage et à la compression des données. Cet en-tête est facultatif. L'unité de données transférée est la **RU** (*Request/Response Unit*).

La couche **DFC** (*Data Flow Control*) gère l'échange des messages entre les EU, la couche DFC assure :

– le contrôle du mode réponse, fonction similaire à celle du bit P/F d'HDLC ;
– le contrôle de l'échange en cas d'utilisation du mode semi-duplex (half-duplex) ;
– le contrôle de flux qui permet la synchronisation des échanges.

Les informations de service de cette couche sont transmises à la couche transmission (TC) pour être incluses dans l'en-tête de celle-ci. La couche contrôle de transmission (**TC**, *Transmission Control*) gère les connexions de transport (session SNA) création, gestion et libération de la connexion de transport. SNA ne connaît que le mode connecté, il n'y a pas de session sans connexion. La couche contrôle de transmission, à l'instar de la couche transport d'ISO, fournit aux couches hautes un canal de transmission fiable quel que soit le sous-réseau de transport physique utilisé. Un en-tête de protocole (**RH**, *Request/Response Header*) est ajouté à l'unité

de données RU pour former une unité de données de base **BIU** (*Basic Information Unit* ou message).

La couche contrôle de chemin (**PC**, *Path Control*) assure la gestion du sous-système de transport. Elle établit le chemin logique entre le NAU origine et destination. La couche PC est subdivisée en trois sous-couches, chacune d'elle assurant une fonction de routage particulière.

L'en-tête TH (*Transmission Heaader*) contient les informations relatives au routage et au contrôle de la congestion du réseau. L'unité de données transférée est la **BTU** (*Basic Transmission Unit*). Pour une meilleure efficacité, des BTU peuvent être regroupées pour former un paquet (**PIU**, *Path Information Unit*).

Les deux autres couches sont similaires à celles du modèle de référence OSI. La couche contrôle de liaison de données utilise **SDLC** (*Synchronous Data Link Control*) tout à fait semblable à HDLC. Cependant, SDLC offre quelques fonctionnalités supplémentaires (gestion du multiligne, gestion des configurations en boucle...).

9.4.4 DSA (Distributed System Architecture) de BULL

Concepts de base

Annoncée en 1976, l'architecture DSA adopte, dès l'origine, une structuration et une répartition des fonctions et services analogues à celles du modèle de référence (figure 9.43). Cette vision a facilité, dès leur stabilisation, l'intégration dans DSA des produits ISO. Les premiers produits compatibles ISO annoncés en 1985 ont été disponibles dès 1986. Les produits ISO FTAM et X.400 ont été livrés sur certains matériels dès 1989.

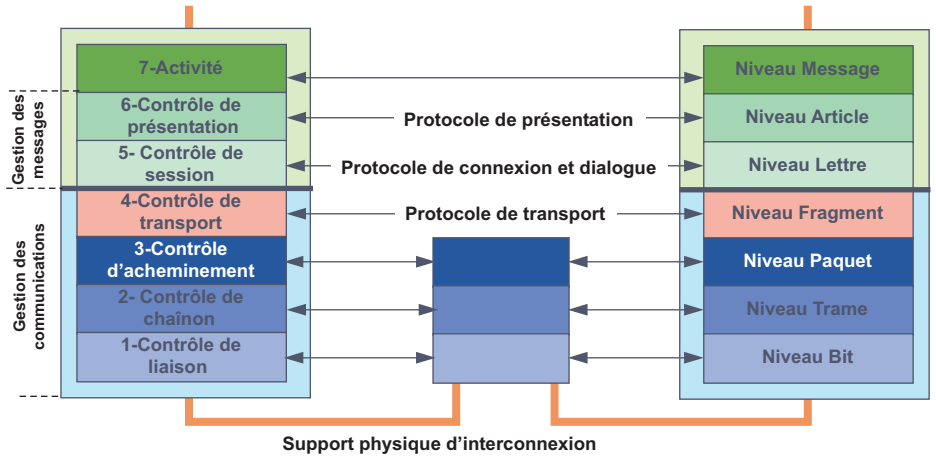


Figure 9.43 Structure du modèle DSA.

Le réseau Bull possède une hiérarchie similaire à celle du réseau IBM, hôtes (machines de type DPSx), contrôleurs de communication (machines de type Datanet 71xx), concentrateurs de terminaux (TCS et TCU) enfin des terminaux (Questar). Le réseau DSA réunissant les Datanet constitue un réseau privé de type X.25 (figure 9.44).

© Dunod – La photocopie non autorisée est un délit

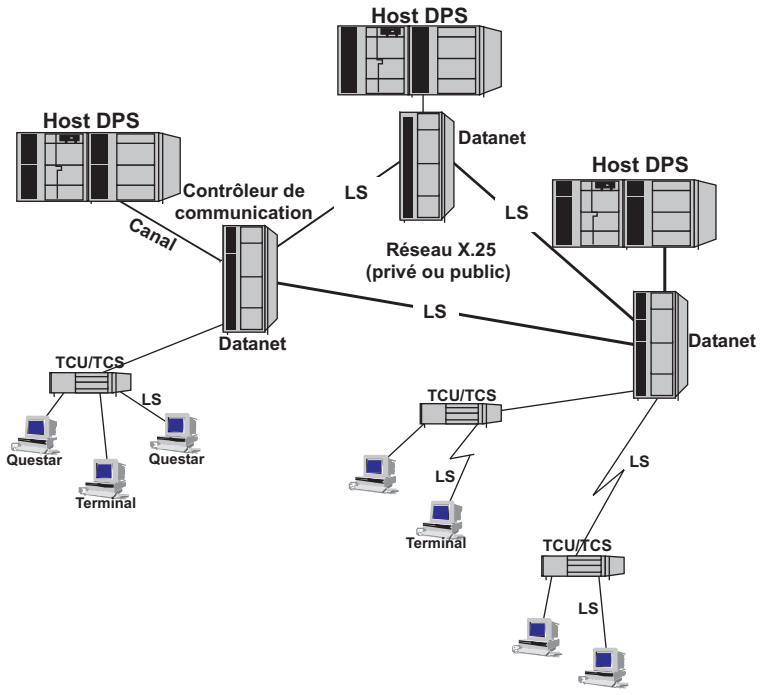


Figure 9.44 Le réseau DSA de Bull.

L'application DSA est une activité, c'est l'usager ou le programme applicatif. Une activité accède au réseau par un point d'accès (**PA**), le point d'accès est identifié par un nom unique dans le réseau. Deux ou plusieurs activités sont mises en relation à travers le réseau via une connexion logique et une boîte aux lettres (*mailbox*) qui est le point d'adressage de l'activité.

Les architectures propriétaire et TCP/IP

L'avenir des architectures propriétaires comme SNA et DSA est fortement lié à leur capacité à évoluer vers les solutions normalisées ou standard (TCP/IP). Il est évident qu'IBM et BULL ne sont pas restés hors de cette évolution, mais ils devront, compte tenu de la base installée, supporter encore longtemps ces architectures.

9.5 CONCLUSION

Aucune architecture n'a pu s'imposer comme étant l'architecture de référence. Les architectures constructeurs trop spécifiques disparaîtront. Le modèle OSI, a certes formalisé les concepts, mais compte tenu de la complexité de ce modèle et donc des difficultés d'implémentation et d'évolution, notamment pour la prise en compte des applications temps réels, il n'a donné lieu qu'à de timides développements. Le modèle de l'IUT s'est imposé pour les couches basses (signalisation hors-bande). Quant à TCP/IP, il semble devenir le modèle fédérateur.

EXERCICES

Exercice 9.1 Fonctions et couches OSI

Quelles sont les couches OSI chargées des opérations suivantes :

a) découpage du flot binaire transmis en trame ;

b) détermination du chemin à travers le réseau ;

c) fourniture de la synchronisation des échanges.

Exercice 9.2 Adresse SAP d'une émission FM

Quelles sont les adresses SAP d'une émission de radio FM ?

Exercice 9.3 Encapsulation

Dans le modèle OSI, est-ce que ce sont les TPDU qui encapsulent les paquets ou le contraire ?

Exercice 9.4 Mode connecté et mode non connecté

Quel est, selon vous, le niveau le plus approprié pour le mode de mise en relation (connecté ou non connecté), et pourquoi ?

Exercice 9.5 Terminal virtuel

Qu'apporte le protocole de terminal virtuel par rapport aux émulations et dans quels types d'application s'impose-t-il ?

Exercice 9.6 Contrôle de flux et transferts isochrones

Peut-on appliquer un mécanisme de contrôle de flux dans un système de communication multimédia (voix, données, vidéo), justifiez votre réponse ?

Exercice 9.7 Contrôle de flux et classe de transport 0

La classe 0 du protocole de transport OSI n'a pas de contrôle de flux, pourquoi ?

Exercice 9.8 Référencement d'une connexion de transport

Pourquoi a-t-on besoin d'identifier les références source et destination dans la partie fixe de la TPDU_CR sachant que les TSAP source et destination sont référencées dans la partie variable ?

© Dunod – La photocopie non autorisée est un délit

Exercice 9.9 Connexion de transport et connexion de session

Énumérez au moins trois similitudes et trois différences entre une connexion session et une connexion transport.

Exercice 9.10 Les types de variables d'ASN-1

Expliquez les différents types de variables ASN–1 pour illustrer les types :

– BOOLEAN
– BITSTRING
– ISO646STRING
– CHOICE
– SEQUENCE.

Puis, définissez une variable de type SET pour illustrer l'utilisation des mots-clés :

– IMPLICIT
– OPTIONAL
– DEFAULT
– NULL

Chapitre **10**

L'architecture TCP/IP

10.1 GÉNÉRALITÉS

10.1.1 Origine

L'architecture TCP/IP a été développée, dans le milieu des années 1970, par la **DARPA** (*Defense Advanced Research Project Agency* – USA –) pour les besoins d'interconnexion des systèmes informatiques de l'armée (**DoD**, *Department of Defense*). TCP/IP, du nom de ses deux protocoles principaux (**TCP**, *Transmission Control Protocol* et **IP**, *Internet Protocol*), est un ensemble de protocoles permettant de résoudre les problèmes d'interconnexion en milieu hétérogène. À cet effet, TCP/IP décrit un réseau logique (réseau IP) au-dessus du ou des réseaux physiques réels auxquels sont effectivement connectés les ordinateurs (figure 10.1).

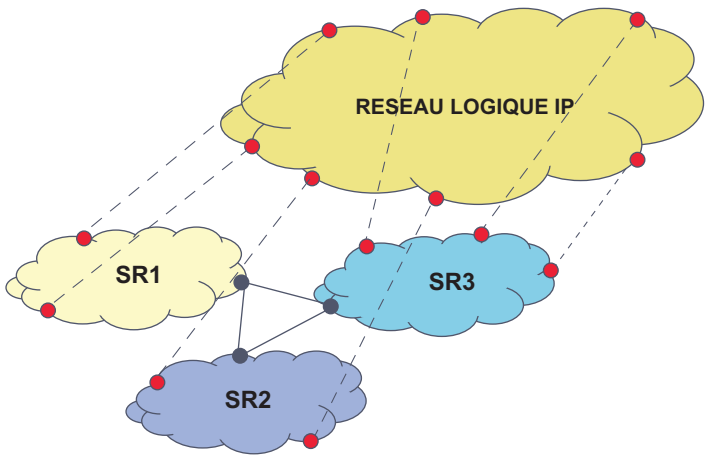


Figure 10.1 Le réseau logique IP et sous-réseaux physiques réels (SR*x*).

Son intégration à UNIX BSD 4, par l'université de Berkeley, en fit le standard de la communauté UNIX (1980). TCP/IP a remplacé (1983) le protocole NCP (*Network Control Program*) dans ARPANET, ancêtre de l'Internet. Aujourd'hui, TCP/IP est le protocole standard de tous les réseaux, du LAN au WAN. De récentes adaptations autorisent les flux multimédia et, en particulier, la voix.

10.1.2 Principe architectural

Précédant le modèle OSI, TCP en diffère fortement, non seulement par le nombre de couches, mais aussi par l'approche. Le modèle OSI spécifie des services (approche formaliste), TCP/IP des protocoles (approche pragmatique). Développé au-dessus d'un environnement existant, TCP/IP ne décrit, à l'origine, ni de couche physique ni de couche liaison de données. Les applications s'appuient directement sur le service de transport. L'architecture TCP/IP ne comprend que 2 couches : la couche transport (TCP) et la couche interréseau (IP). La figure 10.2 compare les deux architectures.

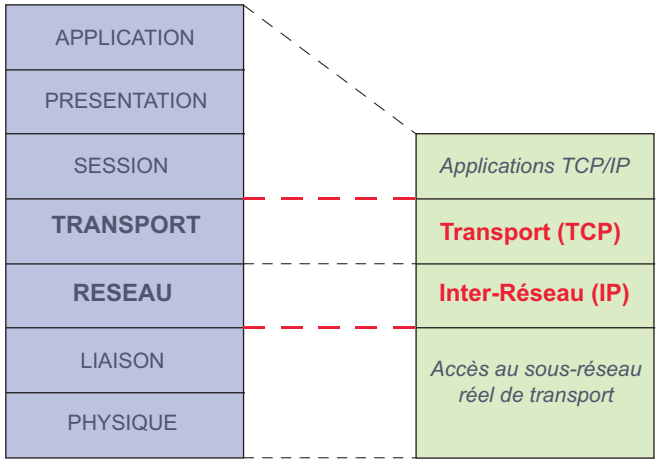


Figure 10.2 Le modèle OSI et l'architecture TCP/IP.

Il n'y a pas de couche application au sens OSI du terme, c'est-à-dire de couche qui présente des « **API** » (*Application Programming Interface*) aux applications, et qui rendent transparent à ces dernières le ou les sous-réseaux réels de transport utilisés. Cependant, un mécanisme particulier, les *sockets*, assure une communication d'application à application en masquant les éléments réseaux.

La couche transport, sur laquelle s'appuient directement les applications, fournit deux types de service : un service en mode connecté (TCP) comparable, en ce qui concerne les services rendus, à TP4 d'ISO et un service de transport allégé **UDP** (*User Datagram Protocol*) qui n'offre qu'un service de type *best effort* (datagramme).

La couche réseau[1] (*Internet Protocol*, IP) présente les mêmes fonctionnalités que la couche réseau d'ISO en mode non connecté (mode datagramme), et les services rendus sont com-

1. Devant répondre à des impératifs militaires, le réseau devait présenter une très grande robustesse à la défaillance d'un nœud. Dans ces conditions, seul le mode non-connecté était approprié.

parables à ceux de la norme ISO IS8473 (couramment appelé CLNP/CLNS, *Connectionless Network Protocol/Connectionless Network Services*).

10.1.3 Description générale de la pile et applications TCP/IP

L'architecture TCP/IP comprend de nombreux programmes applicatifs, utilitaires et protocoles complémentaires (figure 10.3). À l'origine TCP/IP ne spécifiait aucun protocole de ligne, il s'appuyait sur les réseaux existants. L'utilisation massive de TCP/IP a fait apparaître des réseaux tout IP et la nécessité de disposer d'un protocole de liaison (SLIP, PPP). De même, TCP/IP a été adapté aux protocoles dits « Haut Débit » comme le Frame Relay et l'ATM qui constituent aujourd'hui le cœur de la plupart des réseaux privés et d'opérateurs.

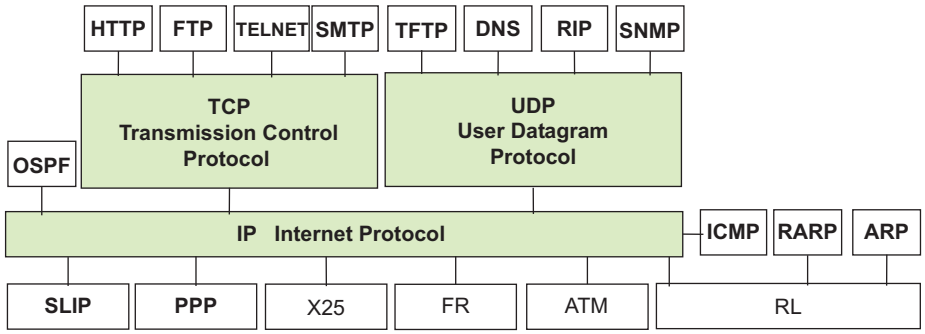


Figure 10.3 Protocoles et applications de TCP/IP.

Les principaux protocoles et applications de l'environnement TCP/IP sont :

- **HTTP**, *HyperText Transport Protocol*, assure le transfert de fichiers hypertextes entre un serveur Web et un client Web ;
- **FTP**, *File Transfer Protocol*, est un système de manipulation de fichiers à distance (transfert, suppression, création...) ;
- **TELNET**, *TELetypewriter NETwork protocol* (ARPA) ou *TERminaL NETwork protocol*, système de terminal virtuel, permet l'ouverture de sessions avec des applications distantes ;
- **SMTP**, *Simple Mail Transfer Protocol*, offre un service de courrier électronique ;
- **TFTP**, *Trivial FTP*, est une version allégée du protocole FTP,
- **DNS**, *Domain Name System*, est un système de bases de données réparties assurant la correspondance d'un nom symbolique et d'une adresse Internet (adresse IP) ;
- **RIP**, *Routing Information Protocol*, est le premier protocole de routage (vecteur distance) utilisé dans Internet ;
- **SNMP**, *Simple Network Management Protocol*, est devenu le standard des protocoles d'administration de réseau ;
- **ICMP**, *Internet Control and error Message Protocol*, assure un dialogue IP/IP et permet notamment : la signalisation de la congestion, la synchronisation des horloges et l'estimation des temps de transit... Il est utilisé par l'utilitaire **Ping** qui permet de tester la présence d'une station sur le réseau.

© Dunod – La photocopie non autorisée est un délit

– **ARP**, *Address Resolution Protocol*, est utilisé pour associer une adresse logique IP à une adresse physique MAC (*Medium Access Control*, adresse de l'interface dans les réseaux locaux) ;
– **RARP**, *Reverse Address Resolution Protocol*, permet l'attribution d'une adresse IP à une station ;
– **OSPF**, *Open Shortest Path First*, est un protocole de routage du type état des liens, il a succédé à RIP ;
– **SLIP**, *Serial Line Interface Protocol*, protocole d'encapsulation des paquets IP, il n'assure que la délimitation des trames ;
– **PPP**, *Point to Point Protocol*, protocole d'encapsulation des datagrammes IP, il assure la délimitation des trames, identifie le protocole transporté et la détection d'erreurs.

10.1.4 Les mécanismes de base de TCP/IP

Le mode de mise en relation

Désirant alléger au maximum la couche interréseau, les concepteurs de TCP/IP n'ont spécifié qu'une couche réseau en mode non connecté (mode datagramme). Ce mode de mise en relation optimise l'utilisation des ressources réseaux mais ne permet d'assurer ni un contrôle d'erreur, ni un contrôle de flux. Au niveau du réseau ces tâches sont reportées sur les réseaux physiques réels. En ce qui concerne les systèmes d'extrémité, c'est la couche TCP qui pallie les insuffisances de la couche interréseau (Internet) en assurant le contrôle d'erreur et de flux de bout en bout (mode connecté). Cette approche est illustrée par la figure 10.4.

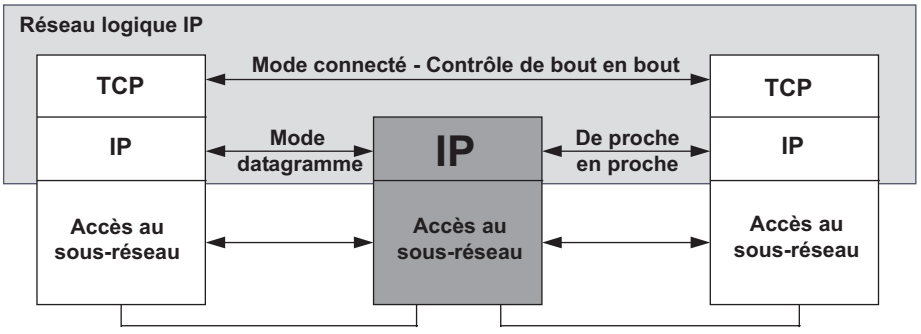


Figure 10.4 Réseau logique IP et modes de mise en relation.

L'encapsulation des données

L'encapsulation consiste à transporter les données d'une couche dans une unité de données de la couche inférieure. Un en-tête contient les informations nécessaires à l'entité homologue pour extraire et traiter les données. Dans le modèle TCP/IP, les données de l'application constituent des messages, ceux-ci sont transportés dans des segments qui seront émis sur le réseau sous forme de datagrammes. L'unité de transport élémentaire est la trame qui constitue au niveau physique un train de bits (figure 10.5).

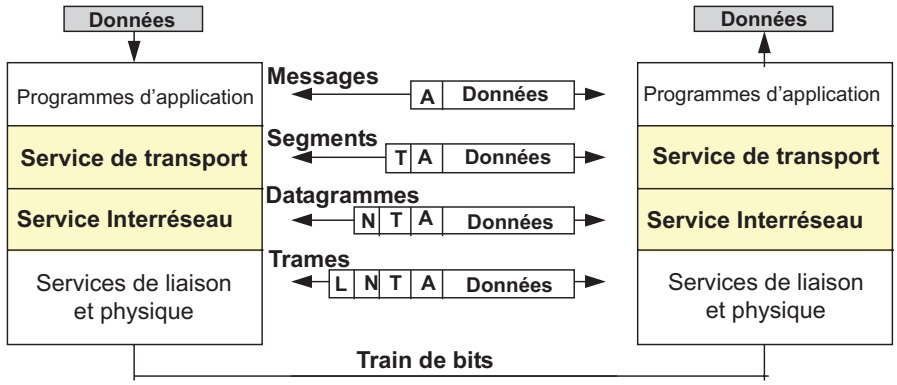


Figure 10.5 L'encapsulation des données dans TCP/IP.

Contrairement à ISO, TCP/IP utilise un format unique d'en-tête de taille fixe. Cette approche, en nécessitant des en-têtes relativement importants, pénalise le débit (*overhead* protocolaire), mais optimise le traitement des blocs de données dans les systèmes intermédiaires. La figure 10.5 illustre ce processus. La terminologie utilisée pour désigner les différents blocs de données diffère quelque peu de celle du monde OSI.

Identification des protocoles

À l'instar d'ISO avec la notion de **SAP** (*Service Access Point*), un adressage de couche organise le dialogue vertical. Chaque unité protocolaire de TCP/IP identifie le protocole ou l'application supérieure. L'**EtherType** des trames « Ethernet[2] » identifie le protocole du niveau réseau. **L'identifiant de protocole** dans le datagramme IP désigne le protocole de transport utilisé et la notion de **port** dans le segment TCP détermine l'instance locale de l'application. La figure 10.6 illustre ce principe et donne quelques exemples d'identifiants normalisés.

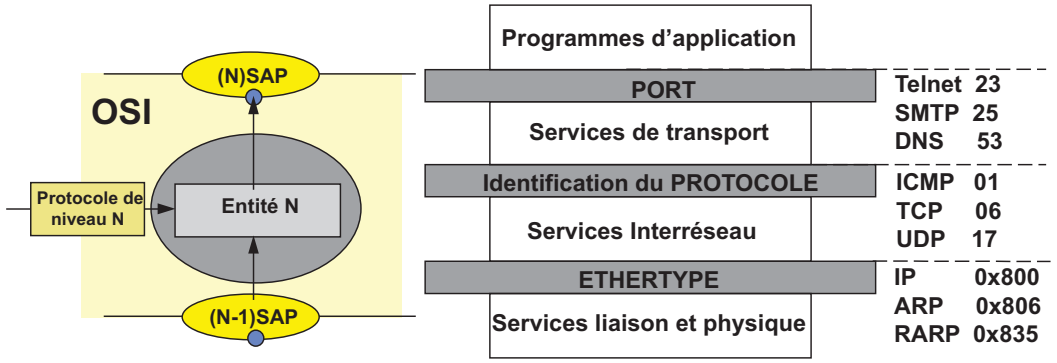


Figure 10.6 Identification des protocoles dans TCP/IP.

2. Ethernet est le nom de marque déposé par XEROX d'un type de réseau local ; ce terme désigne par abus de langage tous les réseaux locaux utilisant le protocole d'accès CSMA/CD.

© Dunod – La photocopie non autorisée est un délit

Taille du segment de données échangé

Chaque réseau, en fonction de ses caractéristiques spécifiques admet des unités de données de taille plus ou moins grande (**MTU**, *Maximum Transfer Unit*). Pour certains réseaux, cette taille est normalisée. C'est le cas, par exemple, pour les réseaux de type Ethernet où la MTU est fixée à 1 500 octets. Dans les réseaux étendus (WAN), la taille est déterminée par l'opérateur en fonction des caractéristiques de ses éléments actifs (buffers...). Un datagramme peut, pour atteindre sa destination, traverser plusieurs réseaux dont les MTU sont différentes. Si le datagramme à transférer a une taille supérieure à la MTU du réseau, le commutateur d'accès devra fractionner (segmenter) l'unité de données pour la rendre compatible avec les capacités de transport du réseau (figure 10.7).

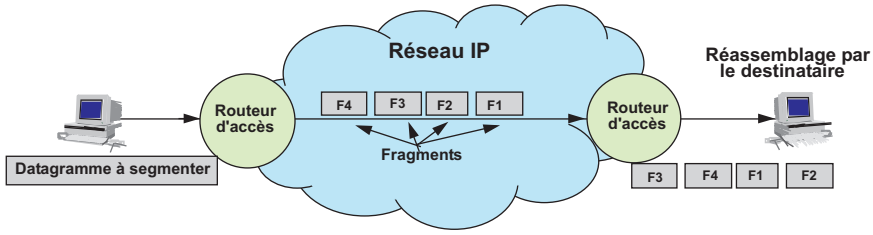


Figure 10.7 Principe de la segmentation sous IP.

Le routage de chaque fragment étant indépendant du précédent et du suivant, aucun nœud n'a la certitude de recevoir tous les fragments, dans ces conditions, seul le destinataire a la capacité de réassembler les différents fragments.

En mode datagramme la perte d'un seul fragment implique une retransmission complète du segment TCP d'origine. Si la connexion est locale, afin d'éviter la reprise d'un segment complet, on cherche à définir une taille de segment correspondant à la taille maximale que peut supporter le réseau. Pour l'interconnexion, via des réseaux de transport, cette taille est fixée à 576 octets, dont 536 utiles. Les passerelles interréseaux doivent être capables de traiter des segments de 576 octets sans avoir à les fragmenter. Néanmoins, cette taille n'est pas nécessairement compatible avec celle admissible par tous les sous-réseaux physiques traversés. Dans ces conditions, la couche IP fragmentera le bloc de données (datagramme IP), chaque fragment constituant un nouveau datagramme IP.

Lors de l'établissement de la connexion de transport, une option de TCP permet l'annonce, et non la négociation, de la taille maximale de segment que le système d'extrémité peut admettre (**MSS**, *Maximum Segment Size*). La figure 10.8 illustre la relation entre MSS et MTU pour la valeur par défaut de 576 octets de MTU. La MTU de 576 octets garantit une charge utile minimale de 512 octets aux données de l'application.

10.1.5 Les instances de normalisation

Plusieurs organismes contribuent à la cohérence des développements des protocoles liés à TCP/IP. Ce sont principalement **l'IAB** (*Internet Activities Board*) qui assure les relations avec les autres organismes de normalisation et définit la politique d'évolution à long terme. L'**IETF**

(*Internet Engineering Task Force*) se préoccupe des évolutions à court et moyen terme. Enfin, l'**IANA** (*Internet Assigned Number Authority*) gère l'attribution d'adresses IP. Des orga-

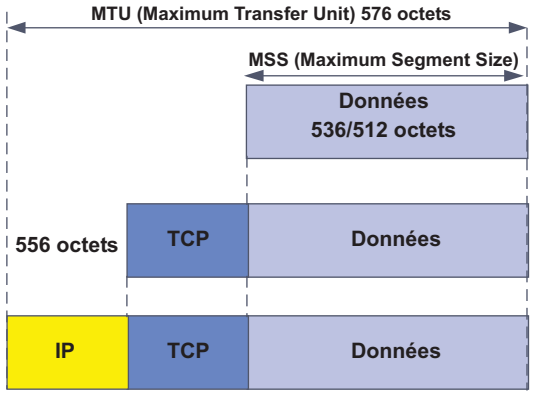


Figure 10.8 Relation entre MTU et MSS (Valeur implicite).

nismes régionaux agissent par délégation de l'IANA, c'est par exemple le **RIPE** (Réseaux IP Européens) représenté en France, depuis le 1er janvier 1998, par l'AFNIC (Association Française pour le Nommage Internet en Coopération). Les standards ou normes TCP/IP sont publiés sous forme de **RFC** (*Request For Comments*). La RFC 1602 décrit le processus d'élaboration (*The Internet Standards Process*).

10.2 L'ADRESSAGE DU RÉSEAU LOGIQUE

10.2.1 Principe de l'adressage IP

Chaque machine (host), raccordée au réseau logique IP, est identifiée par un identifiant logique ou adresse IP (@IP) indépendant de l'adressage physique utilisé dans le réseau réel (figure 10.9). Le réseau logique IP masquant le réseau physique, pour assurer l'acheminement des données, il est nécessaire de définir des mécanismes de mise en relation de l'adresse logique, seule connue des applications, avec l'adresse physique correspondante (résolution d'adresses).

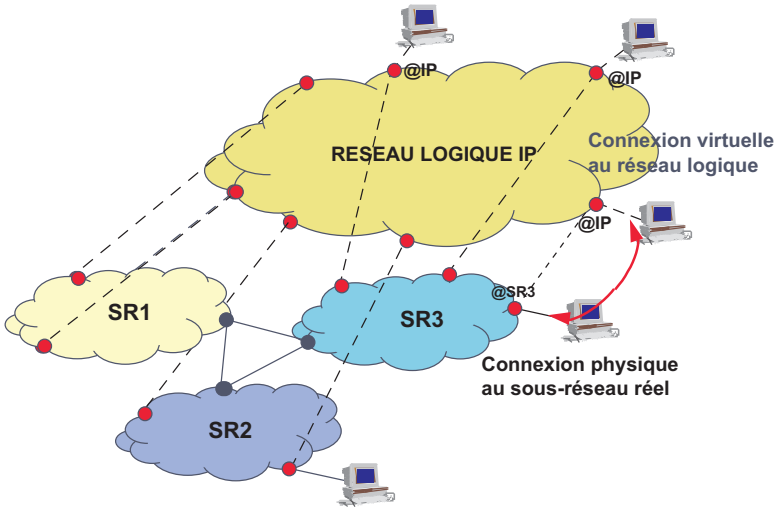


Figure 10.9 Nécessité d'une résolution d'adresses.

© Dunod – La photocopie non autorisée est un délit

Les techniques utilisées pour réaliser la mise en correspondance des adresses diffèrent selon que le réseau supporte ou non la diffusion (réseaux **NBMA**, *Non Broadcast Multiple Access*). Notamment dans les réseaux en mode connecté, l'administrateur réseaux peut être conduit à renseigner manuellement les passerelles[3] interréseaux (table statique, figure 10.10).

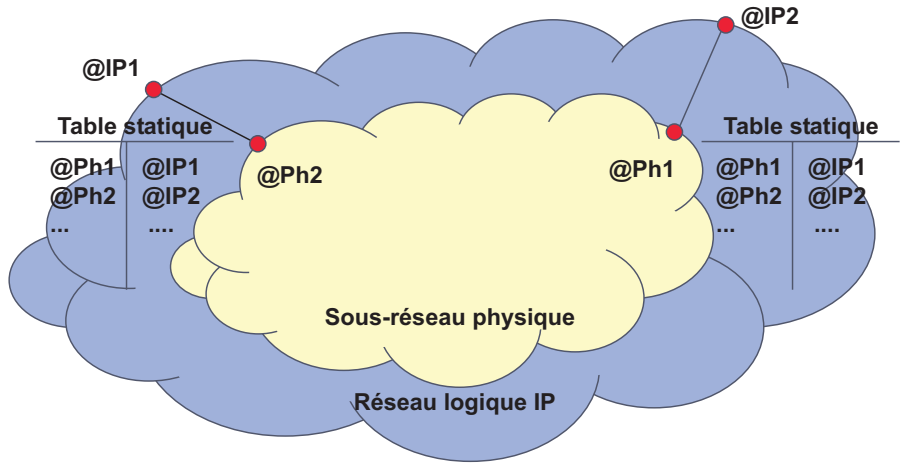


Figure 10.10 Résolution d'adresses dans les réseaux sans diffusion.

Dans les réseaux où la diffusion est réalisable, la machine source diffuse un message du type broadcast (diffusion à tous) pour s'enquérir de l'adresse physique du destinataire. Seul le destinataire, qui reconnaît son adresse IP, répond en indiquant quelle est son adresse physique. L'émetteur mémorise cette correspondance pour une utilisation ultérieure (cache ARP). Ce mécanisme est illustré figure 10.11. Certains protocoles en mode connecté mettent en œuvre des mécanismes de résolution d'adresses en émulant sur un réseau en mode connecté un réseau de diffusion ou en utilisant un serveur d'adresses.

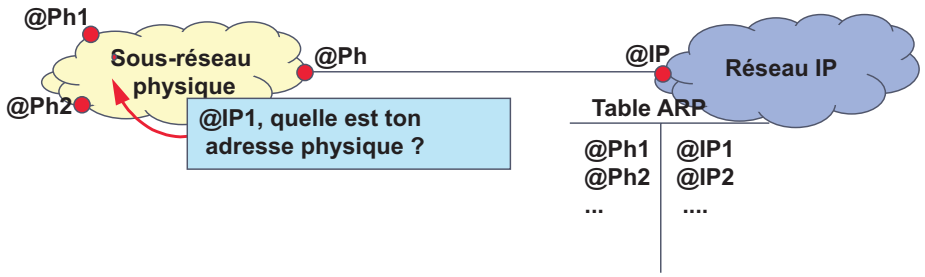


Figure 10.11 Résolution d'adresses dans les réseaux à diffusion.

3. Le terme passerelle sera fréquemment utilisé en lieu et place du terme routeur. En effet, en principe un routeur achemine des données dans un même espace d'adressage, or le nœud d'accès entre le réseau logique et le réseau physique, réalise certes le routage du niveau IP, mais aussi met en correspondance l'adressage IP avec celui du réseau physique utilisé. Il ne s'agit donc pas d'un routeur au sens strict mais plutôt d'une passerelle interréseau.

Enfin, le protocole IP doit assurer le routage dans le réseau logique IP. À cet effet, il doit pouvoir identifier le réseau logique IP concerné (**Net_ID**) et la machine cible (**Host_ID**). L'adressage logique IP ne comporte que ces deux informations (figure 10.12).

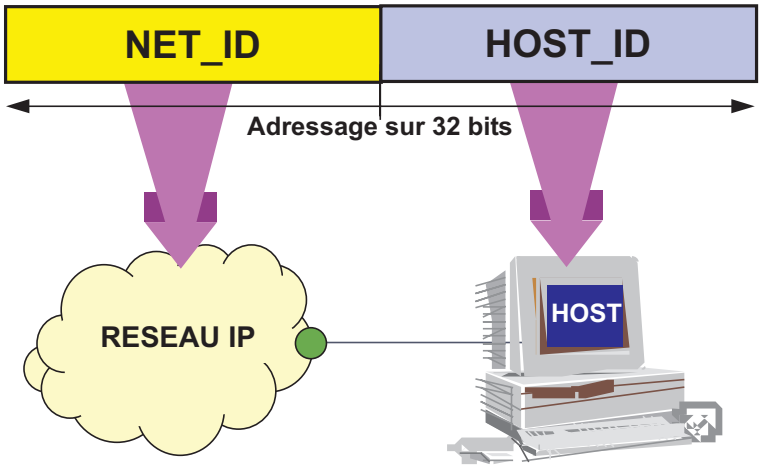


Figure 10.12 L'adressage dans le réseau logique IP.

10.2.2 Les techniques d'adressage dans le réseau IP

Les classes d'adressage

Chaque système, connecté à un réseau IP, a une adresse IP ou numéro IP. Cependant, chaque champ de l'adressage IP est de type à plat, aussi, il n'est pas possible à partir de l'adresse de déterminer la localisation géographique du réseau logique IP.

Limitée à 4 octets (32 bits), on représente l'adresse IP par 4 valeurs décimales séparées par un point[4], la notation est dite décimale pointée (*dotted-decimal notation*). Afin d'assurer une meilleure utilisation de l'espace d'adressage et d'adapter celui-ci à la taille et au besoin de chaque organisation, il a été introduit une modularité dans la répartition des octets entre l'identifiant réseau et l'identifiant machine. Ainsi, 5 classes d'adresse (figure 10.13) ont été définies. Les premiers bits du champ adresse réseau (ID réseau ou Net_ID) permettent de distinguer la classe d'adressage.

Les adresses de classe A s'étendent de 1.0.0.1 à 126.255.255.254. Elles permettent d'adresser 126 réseaux ($2^7 - 2$) et plus de 16 millions de machines ($2^{24} - 2$, soit 16 777 214).

Les adresses de classe B vont de 128.0.0.1 à 191.255.255.254, ce qui correspond à plus de 16 384 réseaux de 65 533 machines. Cette classe est la plus utilisée et les adresses sont aujourd'hui pratiquement épuisées.

La classe C couvre les adresses 192.0.0.1 à 223.255.255.254, elle adresse plus de 2 millions de réseaux (2 097 152) de 254 machines.

4. Certains systèmes UNIX interprètent un zéro devant les chiffres comme indiquant un nombre exprimé en octal. De ce fait, 25 et 025 n'ont pas la même signification, voir commentaires de la figure 10.21.

© Dunod – La photocopie non autorisée est un délit

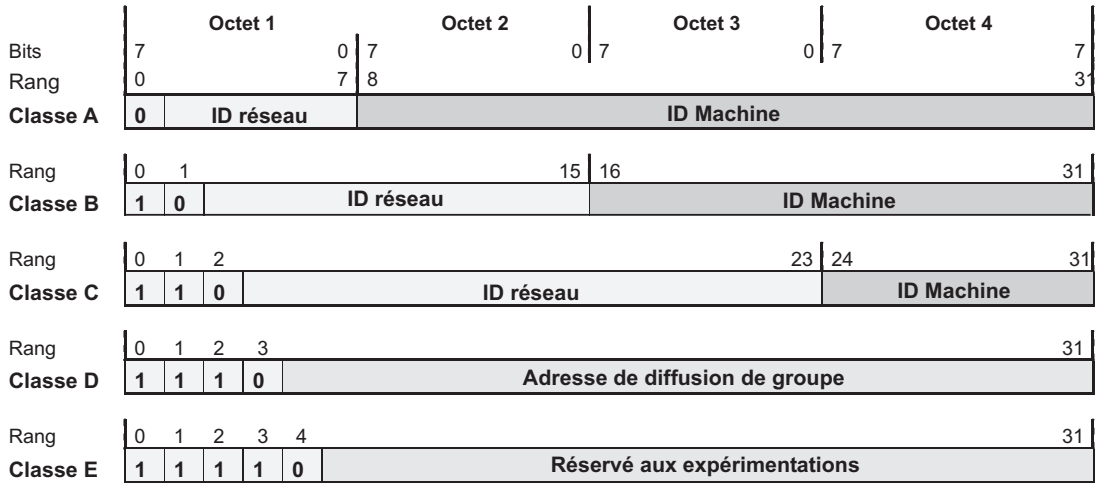


Figure 10.13 Les classes d'adresse IP.

Les adresses de la classe D sont utilisées pour la diffusion (*multicast*) vers les machines d'un même groupe. Elles vont de 224.0.0.0 à 239.255.255.255. Ce groupe peut être un ensemble de machines mais aussi un ensemble de routeurs (diffusion des tables de routage). Tous les systèmes ne supportent pas les adresses de multicast. Enfin, les adresses de la classe E sont réservées aux expérimentations.

Les adresses spéciales

Tout host d'un réseau IP est identifié par le couple <Net_ID><Host_ID>. Certaines valeurs de ces champs ont une signification particulière. C'est ainsi que l'adresse <Net_ID> <0>, où tous les bits du champ Host_ID à zéro, désigne le réseau lui-même[5].

Certaines machines n'ont pas la possibilité de mémoriser une adresse IP. Lors du lancement de cette machine, le système émet une requête pour se voir attribuer une adresse IP (Protocole **RARP**). Durant cette phase d'initialisation, la machine utilise l'adresse 0.0.0.0. Cette adresse ne peut donc pas être affectée à une machine particulière. Dans les routeurs, l'adresse 0.0.0.0 désigne la route par défaut (route à prendre si aucune autre route ne correspond à l'adresse destination).

La machine elle-même ou machine locale peut être auto-adressée avec une adresse de la forme 127. *x*. *x*. *x*, cette adresse dite de boucle locale (*loopback* ou encore *localhost*) est utilisée lors de tests de la machine ou de programmes applicatifs. Tout datagramme émis à destination d'une adresse 127. *x. x .x* est directement recopié du tampon d'émission vers le tampon de réception, il n'est jamais émis sur le réseau, ce qui protège ce dernier d'éventuels dysfonctionnements du nouvel applicatif (figure 10.14).

5. En fait cette adresse correspond à l'adresse de broadcast du système UNIX BSD version 4.2. Elle ne doit jamais être utilisée, si ce n'est pour désigner le réseau lui-même.

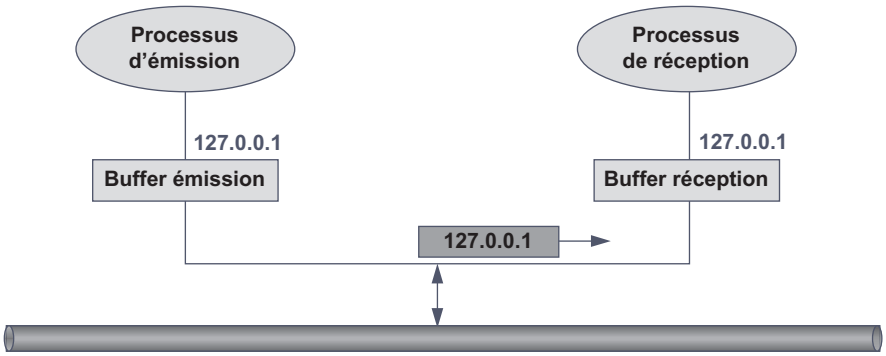


Figure 10.14 L'adresse de boucle locale.

Lorsqu'une machine veut diffuser un message, elle peut, si le message ne s'adresse qu'à un ensemble de machines particulières, utiliser une adresse de multicast dite aussi de diffusion restreinte ou réduite. Si le message doit être adressé à toutes les machines, elle utilisera alors une adresse dite de diffusion générale. On distingue deux types d'adresses de diffusion générale :

– L'adresse 255.255.255.255 utilisée pour envoyer un message à toutes les machines du même segment de réseau. La diffusion est limitée aux seules machines de ce segment, le datagramme n'est pas relayé sur d'autres réseaux. L'adresse 255.255.255.255 est dite adresse de diffusion générale ou limitée.

– Si une machine veut s'adresser à toutes les machines d'un autre réseau, elle utilisera une adresse du type[6] <Net_ID><1>, tous les bits à 1 du champ Host_ID identifient toutes les machines du réseau <Net_ID><0>. Ce message de diffusion est relayé de réseau en réseau pour atteindre le réseau destinataire. L'adresse est dite de diffusion dirigée. Ce principe est illustré figure 10.15.

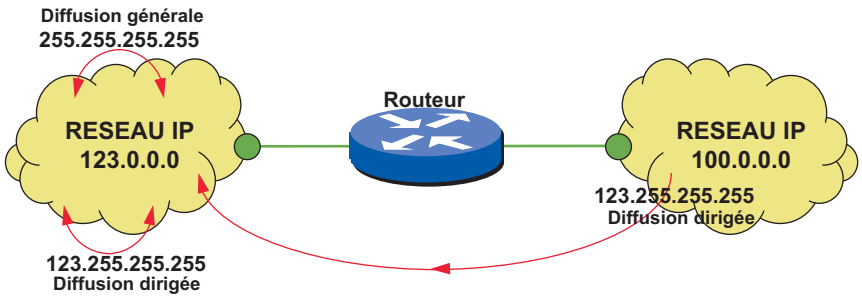


Figure 10.15 Les types de diffusion.

Ainsi :

– l'adresse 123.0.0.0 désigne le réseau d'identifiant 123 ;

– l'adresse 123.0.0.18 désigne la machine 18 du réseau 123

6. Pour simplifier et généraliser l'écriture des adresses nous adopterons la convention d'écriture suivante : <0>, tous les bits du champ concernés sont à zéro ; <1>, tous les bits du champ concerné sont à 1.

© Dunod – La photocopie non autorisée est un délit

– l'adresse 123.255.255.255 est l'adresse de diffusion dirigée à utiliser pour envoyer un message à toutes les machines du réseau 123 ;
– l'adresse 255.255.255.255 est l'adresse de diffusion des machines du même segment de réseau que la machine source.

Adresses publiques et adresses privées

Pour permettre l'interconnexion des réseaux, il faut garantir l'unicité des adresses. C'est l'une des attributions de l'IANA qui attribue à chaque réseau un identifiant unique. Hors, tous les réseaux n'ont pas nécessairement un besoin d'interconnexion via un réseau public, dans ce cas l'unicité d'adresse au plan mondial est inutile. Certaines entreprises (organisations) disposent de leur propre réseau (réseau privé) et n'ont aucun besoin d'interconnexion vers l'extérieur, il est alors possible d'utiliser n'importe quelle adresse IP. Les adresses utilisées dans ce cas sont dites illégales. Par opposition une adresse attribuée par l'IANA est dite légale.

Afin de prévenir une éventuelle anarchie dans l'utilisation des adresses, il a été envisagé de réserver des plages d'adresses à ces réseaux. Ces adresses ne sont pas routables sur le réseau Internet. Elles sont réservées à un usage privé (RFC 1918). De ce fait, elles sont dites adresses privées alors que par opposition les autres sont dites publiques. Le tableau de la figure 10.16 fournit la liste de ces adresses.

Classe	Début de la plage	Fin de la plage	Nombre de réseaux
A	10.0.0.0		1
B	172.16.0.0	172.31.0.0	16
C	192.168.0.0	192.168.255.0	256

Figure 10.16 Les adresses privées (RFC 1918).

Que faire, si un réseau utilisant des adresses de type privé a soudainement des besoins d'accès à un réseau public ? Deux solutions sont envisageables :

– renuméroter toutes les stations avec des adresses publiques ;
– ou réaliser une conversion d'adresses (**NAT**, *Network Address Translator*), c'est-à-dire mettre en correspondance une adresse privée avec une adresse publique.

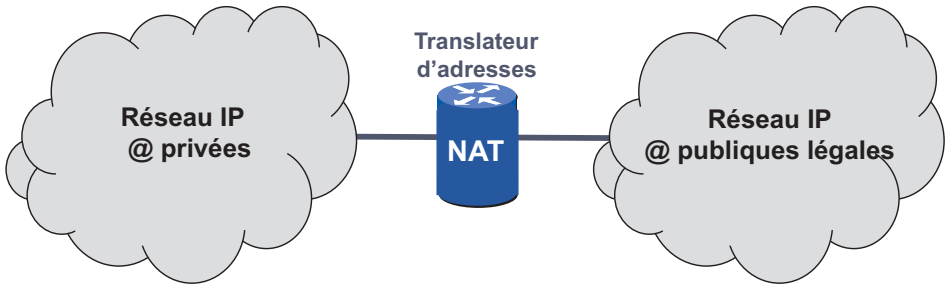


Figure 10.17 Le NAT est l'interface entre un réseau privé et un réseau public.

La seconde solution est généralement adoptée. La passerelle d'accès au réseau public réalisera la translation d'adresses (figure 10.17). La traduction peut être statique, dans ce cas la table de correspondance est renseignée par l'administrateur du réseau, ou dynamique quand la mise en correspondance adresse privée/adresse publique est définie au moment du besoin d'interconnexion. Les adresses publiques peuvent alors être partagées par l'ensemble des machines du réseau privé. La traduction dynamique permet de n'utiliser qu'un nombre restreint d'adresses publiques.

Notions de sous-réseau : le subnetting

➤ Nécessité de définir des sous-réseaux

Supposons une organisation dont les moyens informatiques sont répartis sur deux sites, A et B (figure 10.18). Les tables de résolution d'adresses des passerelles d'accès au réseau physique doivent contenir une entrée par machine du site, alors que l'adresse physique est la même (figure 10.18, site A). Pour alléger cette table et faciliter le routage on pourrait imaginer de doter chaque réseau de site (sous-réseau) d'un identifiant réseau <Net_ID>. Cette approche, non seulement n'est pas rigoureusement conforme à l'approche IP qui consiste à créer d'un seul réseau unique logique IP par organisation, mais de plus est consommatrice d'adresses. Il est préférable de n'attribuer qu'un seul identifiant de réseau (1 seul réseau logique IP par organisation) et de remplacer l'énumération d'adresses IP par un identifiant de site (figure 10.18, site B).

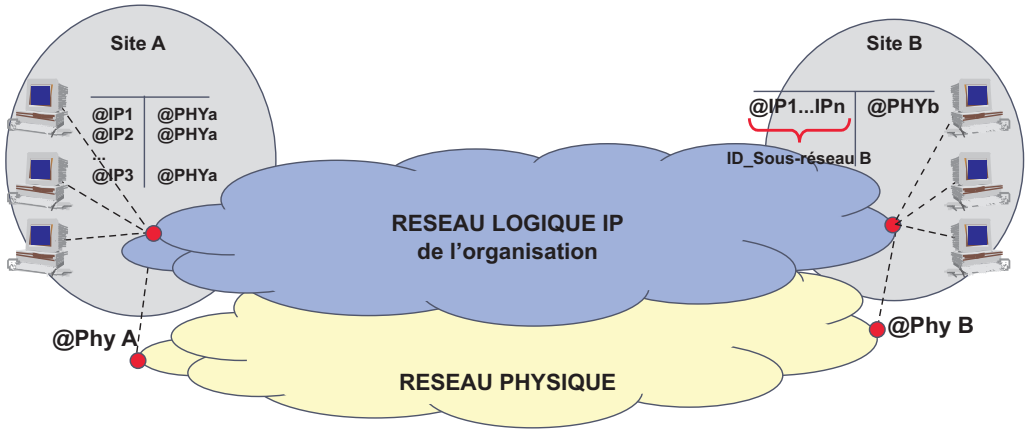


Figure 10.18 Notion de sous-réseaux logiques.

En pratiquant de la sorte on améliore la granularité de l'espace d'adressage. En effet, tout nœud du réseau logique est parfaitement différencié et localisé par un unique identifiant du réseau logique <Net_ID>, l'identifiant du site local ou sous-réseau appelé <SubNet_ID> et enfin le numéro du nœud ou *host* (figure 10.19). La structure originelle de l'adressage IP ne prend pas en compte cette structure d'adresse. Cependant, généralement tous les bits du champ <Host_ID> ne sont pas utilisés pour numéroter les machines, il suffit donc d'en prélever quelques-uns pour identifier le sous-réseau. La taille du <SubNet_ID> sera déterminée en fonction du nombre de sous-réseaux à distinguer.

© Dunod – La photocopie non autorisée est un délit

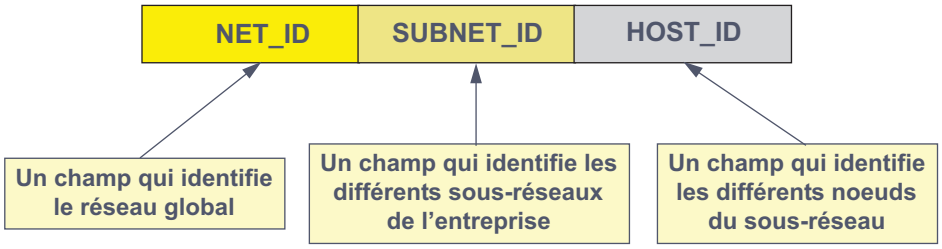

NET_ID
SUBNET_ID
HOST_ID
Un champ qui identifie le réseau global
Un champ qui identifie les différents sous-réseaux de l'entreprise
Un champ qui identifie les différents noeuds du sous-réseau

Figure 10.19 La technique du *subnetting* décompose l'adresse IP en 3 champs.

En principe, l'acheminement est réalisé à partir du champ <Net_ID> dont la taille, dépendant de la classe d'adressage, est connue de chaque routeur. L'utilisation d'un identifiant supplémentaire de longueur variable nécessite d'indiquer à chaque host du réseau quels sont les bits de l'adresse IP à prendre en compte pour définir l'acheminement dans le réseau. Cette information est fournie sous forme d'un champ de bits à 1 appelé **masque de sous-réseau** (figure 10.20).

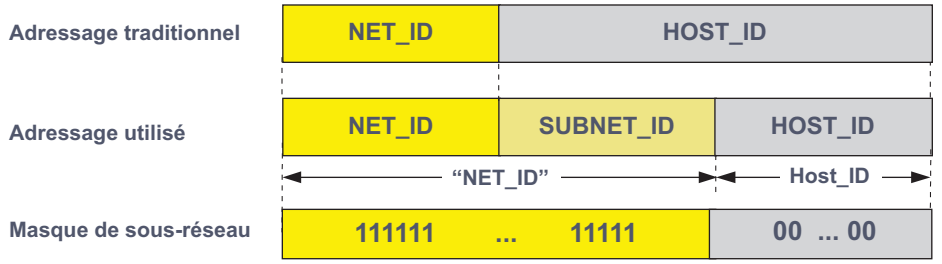


Figure 10.20 Principe du masque de sous-réseau.

Il existe deux méthodes d'écriture des masques de sous-réseaux, qui sont équivalentes :

– Réseau : 10.0.0.0, masque de sous-réseau 255.255.240.0 ;
– ou plus simplement 10.0.0.0/20, le préfixe 20 indique la longueur en bits du masque de sous-réseau (longueur du préfixe réseau ou simplement préfixe). Cette dernière écriture, plus simple, est à préférer à la précédente.

➤ Utilisation du masque de sous-réseau

Lorsqu'une station émet un datagramme à destination d'une autre station, la couche IP locale vérifie, à l'aide du masque de sous-réseau, si le datagramme appartient au même sous-réseau que celui de l'émetteur. Si le datagramme est destiné à une station située sur un sous-réseau distant, le datagramme est envoyé à la passerelle par défaut, charge à celle-ci d'adresser le datagramme vers le bon sous-réseau. Ainsi, une station d'un réseau logique IP doit connaître (figure 10.21) :

– son adresse IP ;
– le masque de sous-réseau ;
– l'adresse de la passerelle locale (routeur).

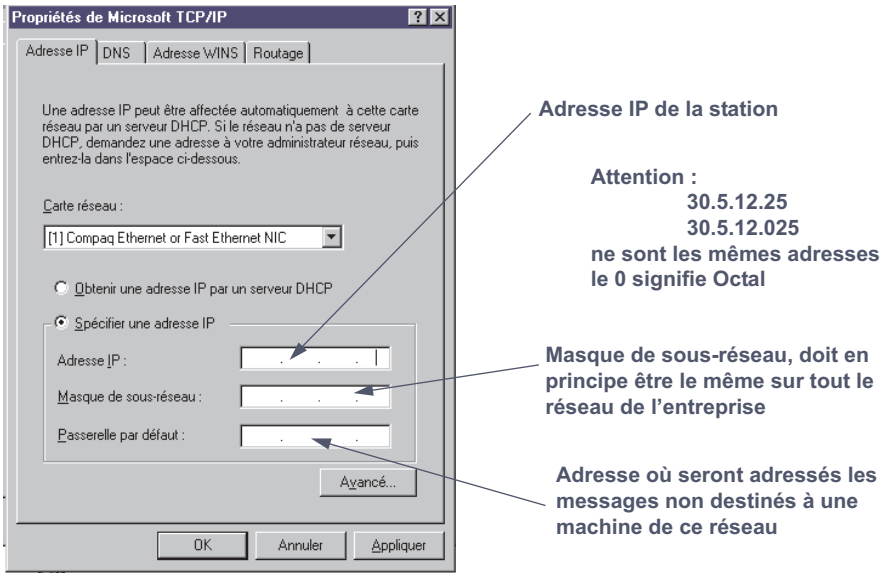

Propriétés de Microsoft TCP/IP
Adresse IP
DNS
Adresse WINS
Routage
Une adresse IP peut être affectée automatiquement à cette carte réseau par un serveur DHCP. Si le réseau n'a pas de serveur DHCP, demandez une adresse à votre administrateur réseau, puis entrez-la dans l'espace ci-dessous.
Carte réseau :
[1] Compaq Ethernet or Fast Ethernet NIC
Obtenir une adresse IP par un serveur DHCP
Spécifier une adresse IP
Adresse IP :
Masque de sous-réseau :
Passerelle par défaut :
Avancé...
OK
Annuler
Appliquer
Adresse IP de la station
Attention :
30.5.12.25
30.5.12.025
ne sont les mêmes adresses
le 0 signifie Octal
Masque de sous-réseau, doit en principe être le même sur tout le réseau de l'entreprise
Adresse où seront adressés les messages non destinés à une machine de ce réseau

Figure 10.21 Informations de configuration d'une machine NT.

Pour déterminer si la machine cible est localisée sur le même sous-réseau, la machine source réalise un « ET » logique entre les bits de l'adresse source et ceux du masque de sous-réseau, elle procède de même avec l'adresse destination. Si le résultat donne une valeur identique les deux machines sont sur le même sous-réseau, sinon le datagramme est adressé au routeur (figure 10.22).

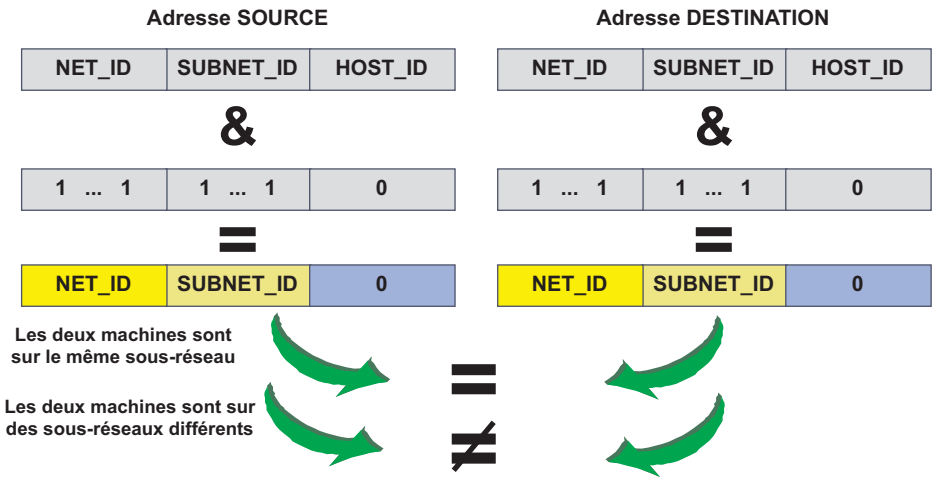


Figure 10.22 Détermination du sous-réseau cible à l'aide du masque de sous-réseau.

© Dunod – La photocopie non autorisée est un délit

➤ Détermination du masque de sous-réseau

Broadcast de sous-réseau

Deux types de broadcast ont déjà été définis, pour prendre en compte les sous-réseaux, il convient d'en ajouter un troisième :

– 255.255.255.255, adresse toutes les machines du réseau sur lequel il a été émis. Ce broadcast ne franchit pas les passerelles (broadcast limité).
– <Net_ID>.<1>, tous les bits du champ <Host_ID> à 1, désigne toutes les machines du réseau <Net_ID>. Ce broadcast, dit broadcast dirigé, est acheminé par les passerelles, sauf configuration spécifique de celles-ci.
– <Net_ID>.<SubNet_ID>.<1>, tous les bits du champ <Host_ID> à 1 adresse toutes les machines du sous-réseau <SubNet_ID>.

L'unicité du masque sur un même réseau

Même si la RFC 1009 autorise, pour un même réseau, l'utilisation de masques de sous-réseaux multiples, cette pratique est à déconseiller. En effet, elle peut introduire des confusions dans l'interprétation des adresses et par conséquent dans l'acheminement. Soit, par exemple, le réseau 10.0.0.0 et le numéro IP 10.1.1.255 :

– si le masque de sous-réseau est 255.255.0.0, cette adresse représente la machine <1.255> du sous-réseau 1.
– mais si le masque de sous-réseau est 255.255.255.0, il s'agit alors de l'adresse de broadcast dirigé du sous-réseau 10.1.1.0.

De même, supposons le réseau de figure 10.23, lorsque l'host <1.8> du sous-réseau 10.1.0.0/16 veut adresser l'host <5> du sous-réseau 10.1.1.0/24, la machine <1.8> considère que son correspondant est situé sur le même sous réseau qu'elle. Ceci est aussi vrai dans l'autre sens.

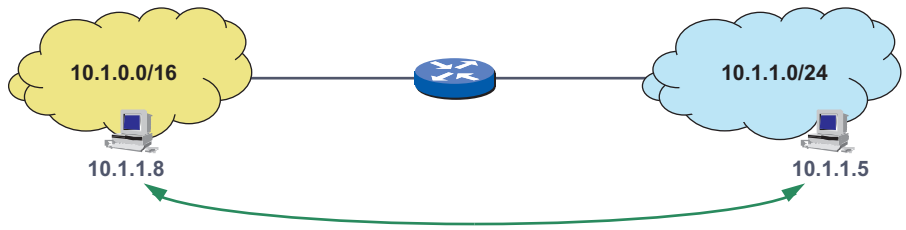


Figure 10.23 Masques de sous-réseaux multiples et problèmes d'acheminement.

Espace de numérotation d'un masque de n bits

Prenons un réseau d'adressage 10.0.0.0/20, le numéro :

– 10.3.0.0 représente-t-il le réseau <10.3> ou le 1er sous-réseau <0> de numéro 10.3.0 ?
– 10.3.255.255 est broadcast dirigé vers l'ensemble des machines du réseau <10.3 > ou un broadcast dirigé, mais limité au seul sous-réseau 10.3.240.0 ?

Dans ces conditions les valeurs tout à <0> et tout <1> du champ <SubNet_ID> sont interdites. La capacité de numérotation (C_n) d'un masque de sous-réseau de *n* bits est de :

$$C_n = 2^n - 2$$

La première conséquence est que pour distinguer deux sous-réseaux il faut au moins 2 bits (figure 10.24) :

Valeur	Ordre du S/R
00	Interdit
01	1er S/R
10	2e S/R
11	Interdit

Figure 10.24 Capacité de numérotation de 2 bits.

Ainsi, les critères à prendre en considération pour la détermination d'un masque de sous-réseau sont :

– l'espace de numérotation des hosts, c'est-à-dire le nombre de machines à numéroter et l'évolution probable de ce nombre (nombre de bits du champ <Host_ID>) ;

– l'espace de numérotation des sous-réseaux, c'est-à-dire le nombre de sous-réseaux à distinguer et l'évolution probable de ce nombre (nombre de bits du champ <SubNet_ID>) ;

– la lisibilité, c'est-à-dire permettre par simple lecture d'identifier facilement le sous-réseau concerné.

L'adressage géographique ou CIDR

Une adresse IP désigne une organisation, elle ne permet pas d'en déterminer la localisation, c'est un adressage à plat. Dans ces conditions, chaque routeur du réseau Internet doit tenir à jour la liste de toutes les adresses attribuées (Net_ID) et la route à suivre. Cet encombrement des tables de routage a conduit, lors de la recherche de solutions pour palier la prévisible pénurie d'adresses, à mettre en œuvre un mécanisme d'affectation géographique des adresses de classe C non attribuées.

D'autre part, il a été décidé de n'attribuer qu'exceptionnellement les adresses de classes B restantes et d'attribuer en lieu et place des adresses contiguës de classe C, de leur faire coïncider une seule entrée dans les tables de routage et de réaliser une affectation géographique. La figure 10.25 indique les plages d'adresses géographiques (RFC 1466).

Ainsi, pour l'Europe les adresses 194 et 195 ont les 7 premiers bits identiques. Il suffit donc d'indiquer aux routeurs que le champ <Net_ID> à prendre en compte est de 7 bits et non de considérer ces adresses comme des adresses de classes C. Une seule entrée suffit alors dans la table de routage. Cette technique, issue de celle du masque de sous-réseau, porte le nom de *supernetting* ou routage interdomaine sans tenir compte de la classe d'adressage (**CIDR**, *Classless InterDomain Routing*).

Le nombre de bits servant à coder la partie commune, ou préfixe d'adresse, est représenté à la fin de l'écriture de l'adresse comme suit : 194.0.0.0/7, ainsi cette adresse indique tous les sous-réseaux européens.

© Dunod – La photocopie non autorisée est un délit

Plage d'adresses	Zone d'affectation
192-193	Divers (adresses déjà attribuées)
194-195	Europe (65 536 réseaux)
196-197	Divers
198-199	Amérique du Nord
200-201	Amérique Centrale et du Sud
202-203	Pacifique
204-205	Divers
206-207	Divers

Figure 10.25 Allocation géographique des adresses de classe C.

10.3 LE ROUTAGE DANS LE RÉSEAU IP

10.3.1 L'adressage d'interface

Supposons le réseau simplifié de la figure 10.26, peu importe le protocole mis en œuvre sur le lien reliant les passerelles d'accès (routeurs IP). Comment la couche IP peut-elle déterminer l'interface de sortie par rapport à une adresse IP destination alors que la couche IP ignore la technologie sous-jacente ?

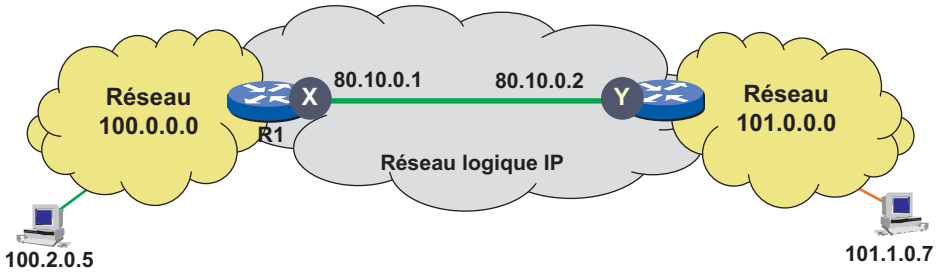


Figure 10.26 Adressage du réseau physique.

En application du principe d'indépendance des couches, le point d'accès au réseau physique ne peut être connu de la couche IP que par une adresse IP. Cette technique d'identification de l'interface d'accès au réseau physique est dite adressage d'interface ou **adressage de LS** (Liaison Spécialisée). Cette méthode garantit l'indépendance des couches. En effet, le routage se réalise d'adresse IP destination à adresse IP d'interface.

Les liens interrouteurs forment ainsi le réseau logique IP. À chaque extrémité est attribuée une adresse IP. Pour comprendre le mécanisme de routage, la figure 10.27 fournit un exemple de configuration d'un routeur[7]. Notons que la route à prendre est désignée par l'adresse distante du lien (*Next Hop*), ce qui correspond à l'adresse du point à atteindre sur le réseau de liens.

7. Le mode de configuration d'un routeur est spécifique à chaque constructeur. Aussi, les exemples ci-après ne constituent qu'une illustration particulière.

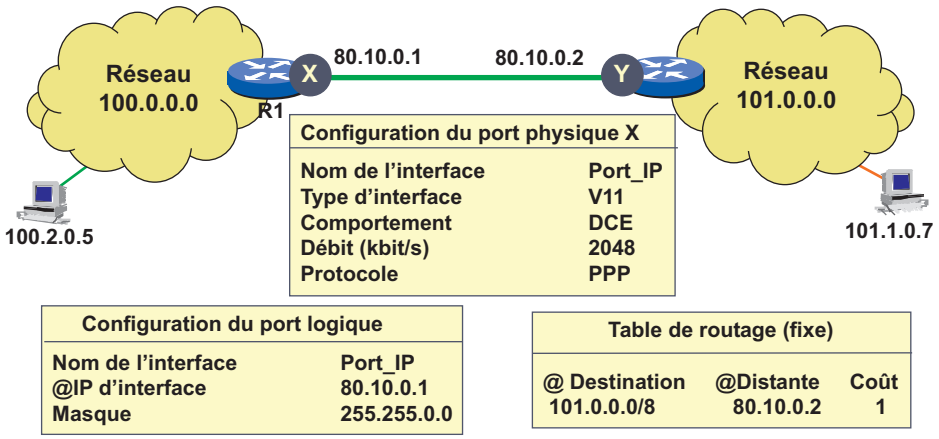


Figure 10.27 Exemple de configuration d'un routeur IP.

10.3.2 Concept d'interface non numérotée

L'attribution d'adresses d'interface est consommatrice d'adresses, aussi la RFC 1812 a-t-elle autorisé le routage sur interface dite non numérotée (*Unnumbered IP*). Un exemple de configuration simplifiée est donné par la figure 10.28. Cette approche viole la règle d'indépendance des couches. Aussi, la RFC 1812 précise que les deux routeurs connectés par une ligne point à point non numérotée ne sont pas à considérer comme deux routeurs mais comme deux demi-routeurs constituant un seul routeur virtuel (figure 10.28).

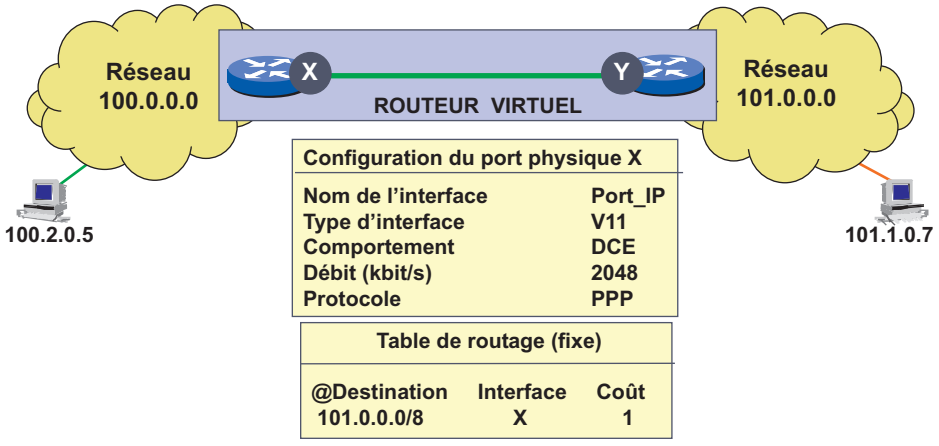


Figure 10.28 Le routage de la RFC 1812.

10.4 LE PROTOCOLE IP ET LES UTILITAIRES RÉSEAUX

10.4.1 Généralités

Rappelons que le protocole IP a pour objectif de masquer les réseaux physiques traversés. N'ayant pas la responsabilité de l'acheminement dans ces réseaux, IP est un protocole réseau

© Dunod – La photocopie non autorisée est un délit

allégé en mode datagramme (figure 10.29), il n'entretient aucune variable d'état. IP n'effectue que les tâches élémentaires d'adaptation de la taille des unités de données aux capacités d'emport du réseau physique traversé (MTU), l'acheminement dans le réseau logique et la désignation des hosts (adresse IP). Ainsi, IP ne réalise aucun contrôle d'erreur, c'est au réseau traversé d'assurer l'intégrité des données qui lui ont été confiées. Il en est de même pour le contrôle de flux du niveau réseau qui peut éventuellement être réalisé par le sous-réseau physique réel.

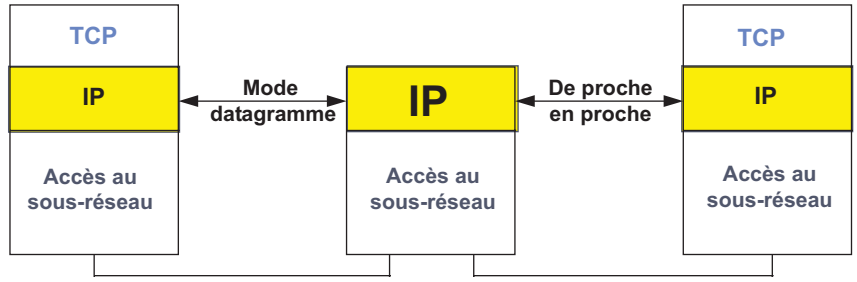


Figure 10.29 Internet Protocol.

10.4.2 Structure du datagramme IP

Un datagramme IP (figure 10.30) peut contenir (champ données) un segment TCP, un message ICMP, ARP, RARP ou encore OSPF.

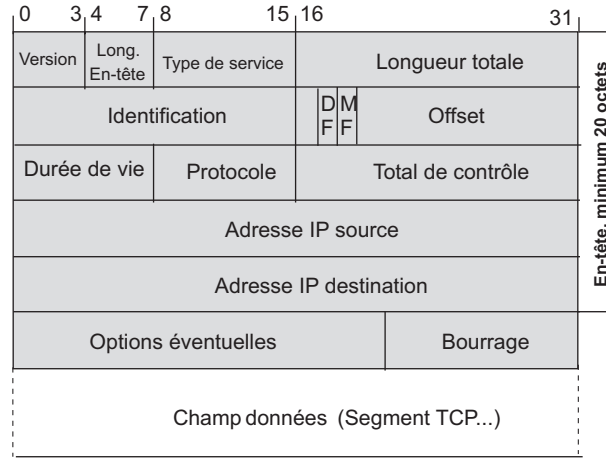


Figure 10.30 Structure du datagramme IP.

Le numéro de version sur 4 bits (**VER**) permet d'identifier le format du datagramme, c'est-à-dire la version du protocole IP utilisé. La présence de cette information autorise la cohabitation de plusieurs versions de protocole dans les systèmes intermédiaires, ce qui est indispensable lors de la mise à jour d'une version du protocole IP. La version courante est la version 4, cependant la version 6 (IPv6) est en cours de déploiement dans l'Internet (voir section 10.8).

Le champ longueur d'en-tête sur 4 bits (**IHL**, *Internet Head Lenght*) indique, en multiple de mots de 32 bits, la longueur de l'en-tête. La valeur courante, lorsqu'aucune option n'est invoquée, est 5 (20 octets).

Le champ type de service sur 8 bits (**TOS**, *Type Of Service*) spécifie, à la passerelle interréseau, le type d'acheminement attendu. La RFC 791 a défini 8 niveaux de priorité et 4 critères d'acheminement (figure 10.31). La plupart des systèmes intermédiaires n'ont pas la possibilité de traiter ces données.

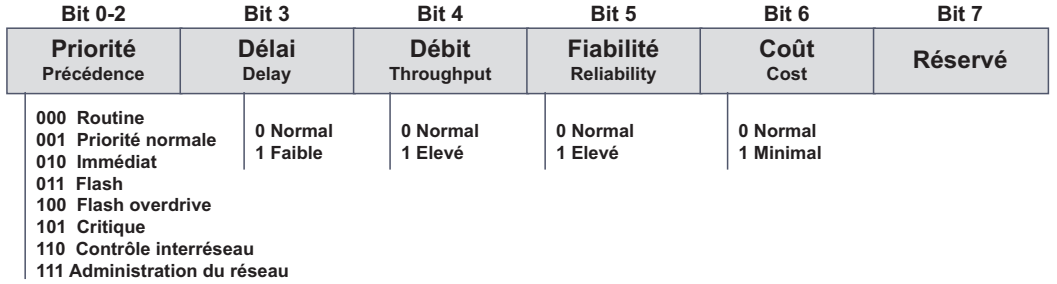


Figure 10.31 Interprétation du champ TOS.

La RFC 1812 (IP *Precedence*) a modifié l'interprétation du champ TOS, en ne spécifiant que les trois premiers bits (figure 10.32).

IP Precedence	Type de trafic
0	Trafic du type Best Effort, grande probabilité d'élimination de datagrammes
1	Best Effort, mais faible probabilité d'élimination de datagrammes
2	Trafic SNA
3-4	Applications critiques, nécessitant une délivrance sans erreur
5	Trafic temps réel (Voix sur IP)
6-7	Trafic des protocoles de routage (mise à jour)

Figure 10.32 IP *Precedence* et type de trafic associé.

La nécessité de développer dans les réseaux un acheminement en fonction d'une certaine qualité de service et donc de différentier les flux a conduit à redéfinir complètement l'utilisation de ce champ (RFC 2474, *Differentiated Services* ou *DiffServ*). Le champ **DS** (*DiffServ*) remplace le champ TOS. Le champ DS comporte 2 sous-champs, DSCP et CU. Le sous-champ **DSCP** (*Differentiated Service Code Point*), sur 6 bits, autorise 64 classes de trafic réparties en trois grandes familles :

– *Assured Forwardind* (AF, RFC 2597) qui comprend 4 classes, elles-mêmes subdivisées. À chaque classe est affectée une priorité différente avec une garantie de bande passante. Des mécanismes spécifiques permettent l'élimination de datagrammes en cas de congestion.

– *Expedited Forwarding* (EF, RFC 2598), défini spécifiquement pour les applications temps réel, minimise le temps de latence dans le réseau. Le réseau prend en compte des contraintes fortes en terme de délai, de gigue (jitter) et de perte.

– *Best effort*, aucun traitement spécifique n'est réalisé. Les datagrammes sont transmis pour le mieux.

© Dunod – La photocopie non autorisée est un délit

Le sous-champ **CU** de 2 bits, actuellement non défini, devrait servir au contrôle de flux.

Le champ longueur totale (**LEN**, *total LENgth field*) sur 16 bits indique la longueur totale, en octets, du datagramme champ en-tête compris. La longueur maximale est de 65 536 octets. Cette longueur maximale est toute théorique, les applications limitent d'elles-mêmes la taille des données utilisateur à 512 octets, ce qui correspond à un MTU de 576 octets.

Le champ identification (**ID**) sur 16 bits : la valeur du champ ID, attribuée par la source, est générée de manière aléatoire par un algorithme initialisé par l'heure système. En cas de fragmentation, l'ID est recopiée par les systèmes intermédiaires dans tous les fragments du datagramme d'origine. L'ID permet, à l'hôte destinataire, d'identifier (N° identification et adresse IP) les différents fragments d'un même datagramme, il facilite ainsi le réassemblage.

Le champ suivant est composé de 3 bits dont le premier n'est pas utilisé. Le bit suivant dit bit **DF** (*Don't Fragment*, ne pas fragmenter) demande au système intermédiaire de ne pas fragmenter le datagramme (bit à 1). Ce bit est utilisé, par exemple, quand le système d'extrémité est incapable de réassembler les différents fragments. Le système intermédiaire qui reçoit un tel datagramme doit soit le router dans sa totalité sur un sous-réseau où le MTU est compatible soit le détruire. En cas de destruction, il en avertit la source par un message ICMP. Enfin, le bit **MF** (*More Fragment*) est positionné à 1 dans tous les fragments d'un même datagramme d'origine pour indiquer qu'un fragment suit. Il est à 0 dans le dernier fragment ou lorsqu'un datagramme n'a pas subit de fragmentation.

Le champ *offset* (13 bits) indique, en cas de fragmentation, la position du fragment dans le datagramme d'origine. Ce champ indique la position du premier bit du fragment dans le datagramme d'origine, en multiple de 8 octets. En conséquence, tous les fragments, sauf le dernier, ont une longueur multiple de 8 (voir section 10.4.3).

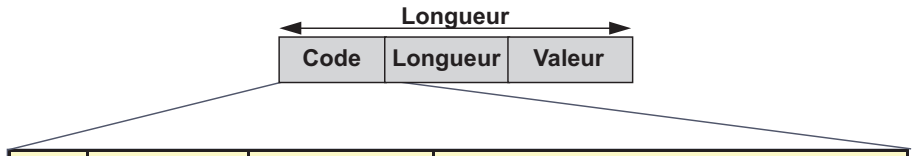
Le champ durée de vie (**TTL**, *Time To Live*) sur 8 bits détermine, en seconde, la durée de vie d'un datagramme. Cette valeur est décrémentée toutes les secondes ou à chaque passage à travers une passerelle. Lorsque le TTL est égal à 0, le datagramme est détruit. La passerelle qui détruit un datagramme envoie un message d'erreur ICMP à l'émetteur. Aucune estampille de temps ne figurant dans l'en-tête IP, les passerelles (routeur) n'ont pas la possibilité de mesurer le temps écoulé, elles se contentent alors de décrémenter ce champ de 1 unité. Le TTL est généralement initialisé à 32 voire 64 (Nombre de sauts[8]).

Le champ protocole (*Protocol*), 8 bits, indique à IP l'origine du champ données (protocole transporté, RFC 1700). Ce champ permet le multiplexage de flux. Quelques exemples de champ protocole ont été donnés dans la figure 10.6.

Le champ total de contrôle (*Checksum*), 16 bits, n'est calculé que sur l'en-tête IP. Le total de contrôle est le complément à 1 de la somme en complément à 1 des données de l'en-tête découpées en mots de 16 bits. Le total de contrôle est recalculé par chaque système intermédiaire (modification du champ TTL et fragmentation éventuelle). La RFC 1141 indique une méthode de calcul simplifiée qui ne tient compte que de la décrémentation de 1 du champ TTL. En cas de fragmentation, le total de contrôle est intégralement recalculé.

8. On considère que toute machine dans l'Internet est accessible en 32 sauts. La valeur de ce champ a été augmentée quand l'Internet a franchi le mur de Berlin et la Grande Muraille de Chine.

Le champ option, de longueur variable, est codé : code option (type), longueur, valeur. Le premier octet, l'octet code, est un champ de bits dont les différentes valeurs et leur signification sont indiquées dans le tableau de la figure 10.33.



Bit	Fonction	Valeur		Commentaire	
0	Copie	0		En cas de fragmentation, l'option n'est pas recopiée.	
		1		L'option est recopiée dans le fragment.	
1-2	Classe Option	00		Datagramme ou supervision de réseau.	
		01		Réservé pour une utilisation future.	
		10		Test.	
		11		Réservé.	
		Classe	Valeur	Longueur	
3-7	Numéro d'option	0	0		Fin de la liste d'options.
		0	1		Alignement d'octet.
		0	2	11	Restrictions de sécurité.
		0	3	var	Routage lâche par la source.
		2	4	var	Horodatage.
		0	7	var	Enregistrement route.
		0	8	4	Identificateur de connexion.
		0	9	var	Routage strict par la source.

Figure 10.33 Codage et options IP.

La longueur du champ option étant variable, celui-ci peut-être suivi de bits de bourrage pour assurer l'alignement de l'en-tête sur des mots de 32 bits. Coûteux en terme de traitement pour les passerelles, le champ option est peu utilisé.

10.4.3 Contrôle de la fragmentation sous IP

La fragmentation d'un segment TCP est contrôlée par les champs : longueur totale (LEN), offset (Offs) dans le segment, et le bit MF du datagramme IP. Le champ offset indique, en multiples de 8 octets, la position du fragment dans le datagramme initial. Le fragment, ainsi constitué, ne peut avoir, pour longueur, que le multiple de 8 le plus proche de la MTU, sauf pour le dernier fragment.

Ainsi, pour une MTU de 128 octets (MTU d'un paquet X.25), la charge utile (niveau IP) ne peut être que de 108 octets (128 - 20 d'en-tête IP), soit une taille effective de 104 octets (13×8), si l'on tient compte de l'en-tête TCP (20 octets), la charge du premier fragment n'est que de 84 octets. La figure 10.34 illustre cette fragmentation pour un segment TCP de 576 octets. Pour faciliter la lecture les valeurs des champs Len et Offset sont exprimées en décimal.

Pour assurer le réassemblage, IP doit attendre l'arrivée de tous les fragments. Les opérations de fragmentation et de réassemblage sont coûteuses en terme de puissance de calcul et de mémoire. De plus, la perte d'un seul fragment provoque une reprise par la couche TCP du segment fragmenté.

© Dunod – La photocopie non autorisée est un délit

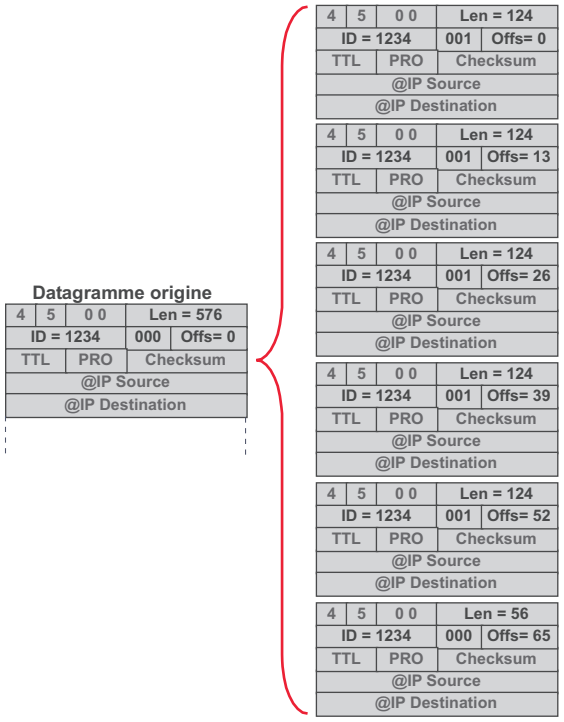


Figure 10.34 Fragmentation d'un segment TCP.

10.4.4 Le protocole ICMP

Le protocole ICMP (*Internet Control Message Protocol*, RFC 792) permet d'informer d'une erreur réseau (message d'erreur) ou de formuler une demande d'état à un système (message d'information). Les messages ICMP sont encapsulés dans un datagramme IP (Protocole = 1). La figure 10.35 représente la structure du message ICMP et fournit quelques exemples de codage des différents champs.

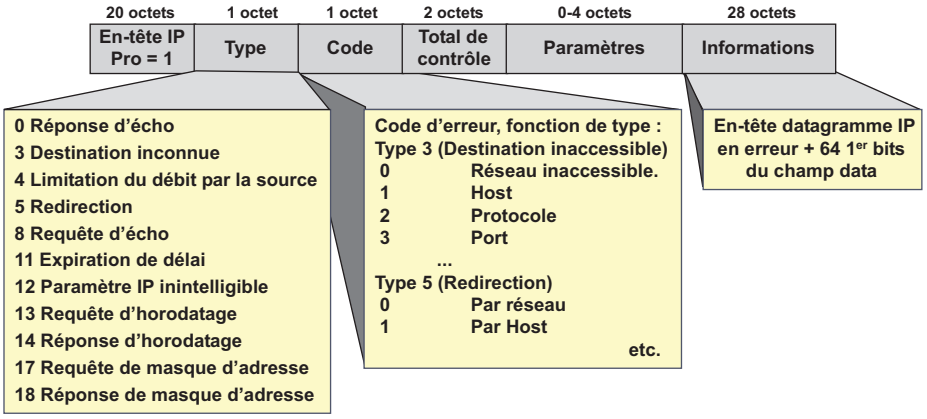


Figure 10.35 Structure du message ICMP.

Le protocole ICMP ne fiabilise pas IP, c'est un protocole d'information. Les différentes fonctions sont aussi utilisées par des utilitaires. Par exemple, la commande PING (voir section 10.4.5) utilise les messages de demande de réponse d'écho (type 0, 8). Le protocole **NTP** (*Network Time Protocol*) utilise la commande ICMP Timestamp (type 13, 14) pour synchroniser les horloges du réseau. Les estampilles temporelles sont exprimées en milliseconde depuis minuit TU (Temps Universel).

10.4.5 L'utilitaire PING

L'utilitaire **PING** (*Packet INternet Groper*) permet de tester l'accessibilité d'un système et d'évaluer le temps aller et retour entre le système source et le système cible. La commande PING envoie un message ICMP de demande d'écho vers la machine cible, celle-ci retourne une réponse d'écho (figure 10.36).

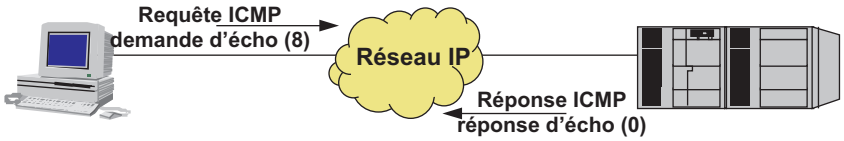


Figure 10.36 Principe de la commande PING.

La commande PING permet de tester une liaison TCP/IP de bout en bout, et, ainsi, de déterminer un éventuel élément défaillant :

- PING sur l'adresse 127.0.0.1 teste l'installation de la pile TCP/IP sur la machine source.
- Sur l'adresse IP de la machine source, PING permet de vérifier que cette station est correctement configurée.
- Sur l'adresse de la passerelle par défaut, PING permet de contrôler la validité du masque de sous-réseau et la configuration de la passerelle par défaut.
- PING sur l'adresse de l'interface de sortie (LS locale) valide la configuration de cette interface.
- Sur l'adresse de LS distante, PING s'assure que le lien WAN est établi et que le routeur local et distant sont correctement configurés vis-à-vis du réseau source.
- PING sur l'adresse de station distante valide la configuration de bout en bout.
- Enfin, PING avec un nom d'hôte vérifie que le fichier « host » local ou que le serveur DNS est correctement renseigné.

La structure du message ICMP d'écho utilisé par la commande PING est donnée en figure 10.37.

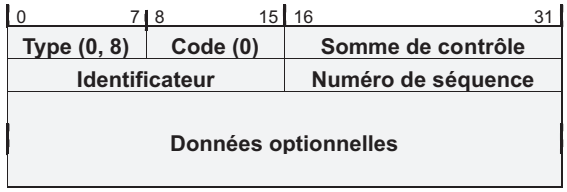


Figure 10.37 Structure du message d'Echo utilisé par l'utilitaire PING.

© Dunod – La photocopie non autorisée est un délit

Le numéro de séquence est initialisé à zéro et incrémenté à chaque envoi d'un datagramme PING. Le champ identificateur permet au système source de différentier les réponses d'une séquence de PING vers des systèmes différents. La réponse à une commande PING doit parvenir dans un délai maximal de 20 secondes, sinon la cible est déclarée inaccessible.

10.4.6 La résolution d'adresses

Généralités

Les applications ne connaissent que l'adresse logique IP, alors que les données sont acheminées dans le réseau physique. Pour masquer aux applications l'adresse physique du réseau d'acheminement, la couche IP doit établir une correspondance entre l'adresse logique et l'adresse physique. Ce mécanisme s'appelle **mécanisme de résolution d'adresses**.

La résolution d'adresses dans les réseaux à diffusion

Le protocole **ARP** (*Address Resolution Protocol*) permet à un host ou à une passerelle d'obtenir l'adresse MAC du nœud d'un réseau local auquel il doit adresser des données. La figure 10.38 illustre le mécanisme. L'host d'origine ignore l'adresse physique de son correspondant (résolution intraréseau). Il émet une demande de résolution d'adresses sur le réseau physique à destination de la machine cible. Cette demande est encapsulée, dans une trame MAC (Ethernet, Token Ring...) dont le champ adresse destination est à FF-FF-FF-FF-FF-FF (adresse de diffusion). Tous les nœuds connectés au réseau local, reconnaissant une demande ARP extraient l'adresse MAC origine et l'adresse IP origine. Cette correspondance est stockée, pour une utilisation ultérieure, dans une table dite cache ARP. Seule, la machine qui a reconnu son adresse logique répond en fournissant son adresse physique. La réponse est stockée dans le cache ARP de la machine origine.

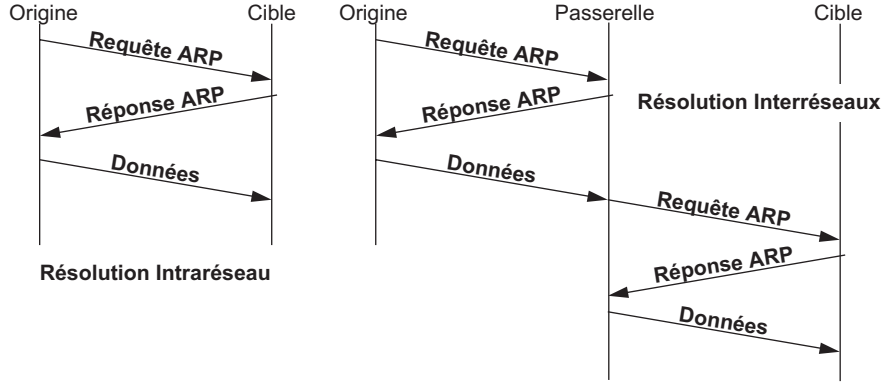


Figure 10.38 Mécanisme de la résolution d'adresses.

Lorsqu'une machine doit envoyer un datagramme à une machine appartenant à un autre réseau (résolution interréseaux), la résolution s'effectue en deux temps. La machine origine réalise une première résolution d'adresses avec la passerelle, puis adresse les données à la passerelle qui elle-même émet une requête ARP sur le réseau destinataire pour connaître l'adresse MAC de la machine cible. Enfin, les données sont adressées à la machine cible.

Lorsque la machine origine ne connaît pas l'adresse logique de la passerelle, elle émet sa requête directement sur le réseau. La passerelle qui reconnaît l'adresse IP d'un hôte qu'elle sait joindre répond avec sa propre adresse physique (MAC adresse). La passerelle doit être configurée pour répondre à ce type de demande (Proxy-ARP).

Pour limiter le trafic de résolution d'adresses et éventuellement détecter une duplication d'adresses, toute machine s'envoie, lors de sa mise sous tension, une demande ARP (*gratuitous ARP*). La figure 10.39 illustre le format d'un paquet ARP.

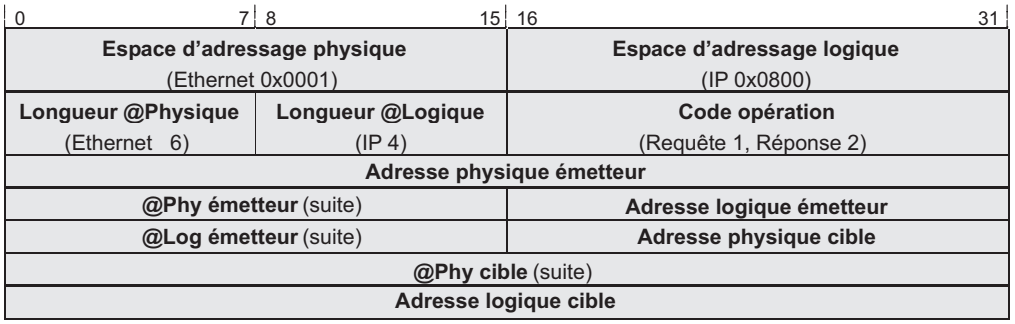


Figure 10.39 Structure du datagramme ARP.

À l'inverse du protocole ARP, le protocole **RARP** (*Reverse Address Resolution Protocol*) permet à une station qui ne dispose pas d'adresse IP (station sans disque, imprimante...) de s'en voir attribuer une. Le format du paquet RARP est identique à celui du protocole ARP. Seule, la valeur du champ code opération est différente : 3 pour une requête et 4 pour la réponse. Une machine du réseau doit être configurée pour répondre à ces requêtes (serveur RARP). Le protocole RARP est aujourd'hui considéré comme obsolète.

La résolution d'adresses dans les réseaux NBMA[9]

Dans les réseaux sans diffusion, la résolution peut être statique, la table de correspondance est alors renseignée par l'administrateur (résolution statique) ou réalisé par un protocole particulier (résolution dynamique) comme dans les LAN ATM. Les techniques LAN ATM consistent à émuler sur un réseau ATM un réseau local. Par exemple, la RFC 1577 ou *Classical IP* (**CLIP**) définit un réseau IP sur un réseau physique ATM comme un sous-réseau logique (**LIS**, *Logical IP Subnetworking*). Un LIS est un ensemble de machines IP connectées à un réseau ATM partageant un même préfixe d'adresse IP.

Les stations d'un même sous-réseau (LIS) communiquent directement entre elles après avoir établi un circuit virtuel. Pour cela, chaque station doit connaître les adresses IP et ATM du destinataire. La fonction de résolution d'adresses est assurée par un serveur d'adresses (serveur ATMARP) qui, sur sollicitation d'une requête **ATMARP** (*ATM Address Resolution Protocol*), renvoie l'adresse ATM correspondante. Chaque réseau logique (LIS) possède une machine configurée en tant que serveur ATMARP (figure 10.40). Lors de la configuration d'un client LIS celui-ci, outre son adresse ATM, est informé de l'adresse ATM du serveur ATMARP.

9. **NBMA**, *Non Broadcast Multiple Access*.

© Dunod – La photocopie non autorisée est un délit

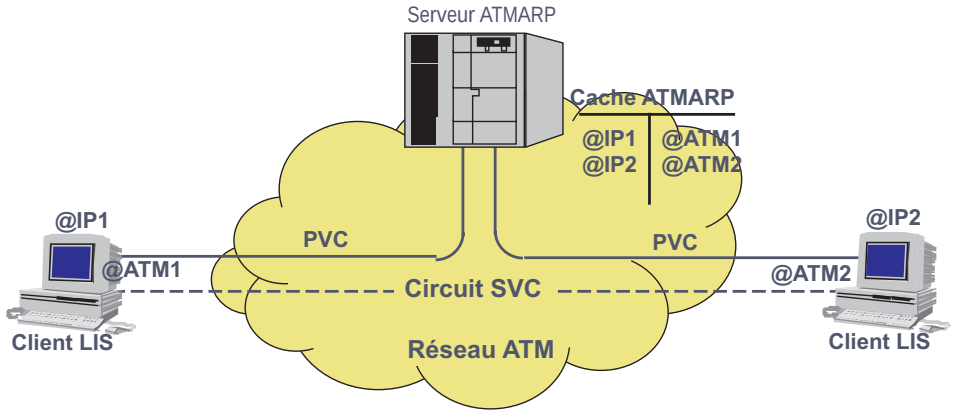


Figure 10.40 Réseau LAN ATM dit Classical IP.

La figure 10.41 décrit le scénario de résolution d'adresses de ce type de réseau. Lors de sa mise sous tension, le client LIS établit un circuit virtuel avec le serveur ATMARP. Ce dernier émet, vers cette station, une requête **InARP** (*Inverse ARP*) pour apprendre son adresse IP. Le serveur ATMARP met alors son cache ARP à jour (table de correspondance @IP/@ATM).

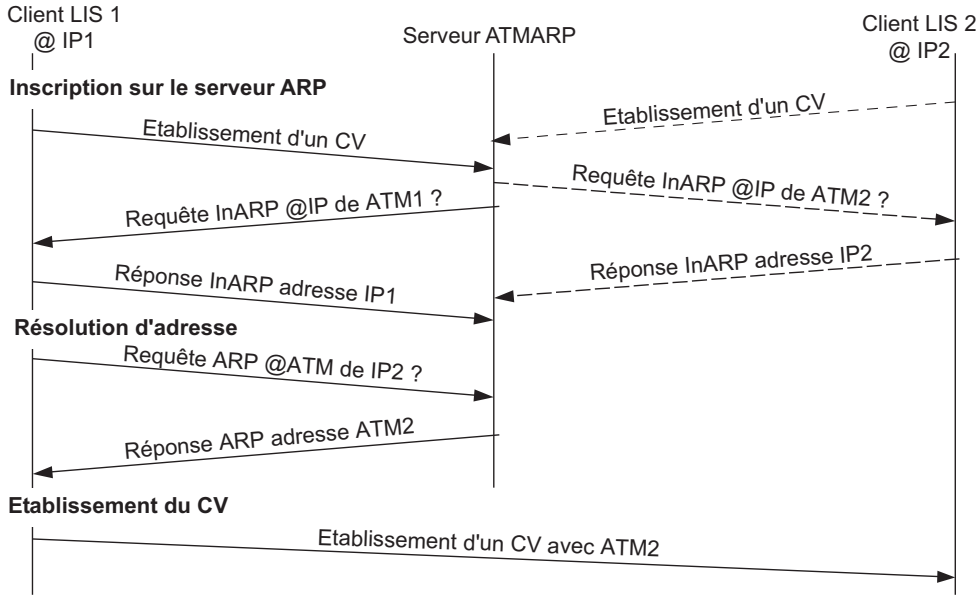


Figure 10.41 Établissement d'un circuit virtuel entre deux clients LIS.

Lorsqu'un client LIS veut entrer en relation avec un autre client du même LIS, il émet une requête ARP vers le serveur ATMARP (quelle est l'adresse ATM de la station IP ?), celui-ci lui fournit alors l'adresse ATM, le client LIS met son cache ATM à jour (@IP/@ATM), et établit un circuit virtuel avec cette station.

10.4.7 Les utilitaires de configuration

Généralités

Le protocole RARP permet à une station de se voir attribuer une adresse IP, les requêtes RARP utilisent une adresse de broadcast limité. De ce fait, elles ne sont pas retransmises par les routeurs, ce qui implique un serveur RARP par réseau (sous-réseau). Le masque de sous-réseau peut-être découvert par une requête ICMP. Mais, ce sont les seules informations que la machine peut obtenir. Le protocole **BOOTP** (*BOOTstrap Protocol*) permet à une machine sans disque de connaître l'intégralité des paramètres de configuration du réseau (adresse, masque, passerelle par défaut...). Le serveur BOOTP associe à l'adresse physique du client un profil. De ce fait, BOOTP n'est utilisable que dans un environnement relativement figé, ce qui en limite l'utilisation notamment avec l'introduction du concept de mobilité (ordinateurs portables). **DHCP** (*Dynamic Host Configuration Protocol*), considéré comme une évolution de BOOTP, autorise une configuration automatique des stations et permet la mobilité.

B00TP

Le serveur de BOOTP ne fournit au client que le nom du fichier de boot à télécharger. Ce fichier pouvant être éventuellement une image mémoire complète du système. Les machines utilisant BOOTP, par exemple les stations XWindows (X.11), n'ont besoin en mémoire morte (ROM) que d'un système réduit comportant au minimum une pile IP/UDP, les utilitaires BOOTP et **TFTP** (*Trivial File Transfer Protocol*).

La requête BOOTP est émise en broadcast (255.255.255.255) ; un routeur, configuré en agent relais (proxy), propage éventuellement la requête aux serveurs BOOTP situés sur d'autres segments du réseau.

Si le client BOOTP connaît son adresse il la précise, sinon il utilise l'adresse 0.0.0.0, de même, le client peut connaître le nom du fichier de configuration, dans ce cas il fournit le nom du fichier recherché. Par défaut, le serveur BOOTP renvoie l'adresse IP affectée au client, le nom du fichier de configuration et l'adresse de la machine où est stocké le fichier à télécharger, cette machine pouvant être le serveur BOOTP lui-même. Il reste alors au client à se connecter à cette machine pour télécharger, à l'aide de TFTP, le ou les fichiers nécessaires à son fonctionnement (système, logiciels...), cette procédure est appelée démarrage en deux temps.

BOOTP utilise IP et UDP, il doit donc assurer lui-même la fiabilisation de la transmission. Pour ce faire, il utilise le total de contrôle de UDP et assure les reprises sur temporisation. Pour soulager le travail du client, le bit DF du datagramme IP est positionné à 1 (ne pas fragmenter).

DHCP

Reprenant les principes de BOOTP, DHCP (RFC 1541) offre de véritables fonctions de configuration automatique des stations. Contrairement à BOOTP qui affecte de manière statique une adresse IP, le serveur DHCP détient un jeu d'adresses valides et les paramètres associés de configuration IP qui sont alloués dynamiquement aux clients DHCP. Les stations configurées par DHCP libèrent les adresses lorsqu'elles n'en ont plus besoin. DHCP propose trois mécanismes d'adressage :

© Dunod – La photocopie non autorisée est un délit

– L'allocation manuelle, à l'instar de BOOTP ou RARP, DHCP alloue une adresse spécifique à un client. L'administrateur gère donc les adresses IP.
– L'allocation automatique permet, lors d'une configuration initiale, d'attribuer automatiquement à une station une adresse IP choisie par le système parmi un pool d'adresses. La station conserve cette adresse tant qu'elle n'a pas été libérée explicitement par l'administrateur.
– L'allocation dynamique, dans ce mode de fonctionnement, DHCP alloue temporairement (bail) une adresse IP. En fin de bail, la machine peut en demander le renouvellement.

La figure 10.42 décrit les différentes étapes d'une configuration automatique DHCP. La station, à l'initialisation, diffuse un message d'exploration (**DHCPDiscover**). Tous les serveurs DHCP actifs sur le réseau formulent une offre de service (**DHCPOffer**). La station cliente passe alors dans l'état sélection. Lorsque la station a choisi un serveur DHCP (serveur élu), elle formule auprès de celui-ci une requête d'affectation d'adresses (**DHCPRequest**).

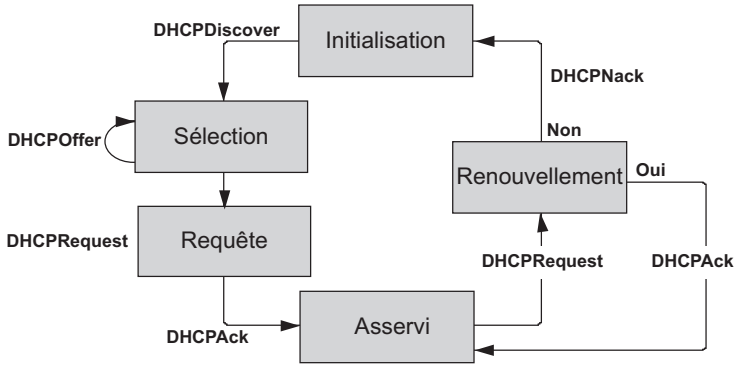


Figure 10.42 Différents états d'un client DHCP.

Le serveur DHCP sélectionné accuse réception de la requête (**DHCPAck**) en fournissant les éléments de configuration TCP/IP nécessaires à la station (adresse IP, masque de sous-réseau, adresse de la passerelle...) et la durée de validité de ces paramètres (bail). La station est alors dans l'état asservi. Si elle en a la possibilité, elle mémorise les informations. Elle pourra les utiliser, lors des connexions futures, jusqu'à expiration du bail, échéance au bout de laquelle elle formulera une demande de renouvellement (**DHCPRequest**). La requête initiale ou le renouvellement peuvent être refusés par le serveur élu (**DHCPNAck**). La station est alors revenue à l'état initialisation.

Le message **DHCPRelease** permet au client de résilier son bail avant l'échéance de celui-ci. Le message **DHCPDecline** est utilisé par le client pour informer un serveur que son offre est invalide. Enfin, le message **DHCPInform** permet à une machine d'obtenir des paramètres de configuration supplémentaires. DHCP utilise les mêmes ports et le même format de message que BOOTP, seul le dernier champ est différent.

10.4.8 Conclusion

Les limitations de l'adressage, dues essentiellement à la structure à plat de l'adressage IP, conjuguées au succès d'Internet ont contribué à la pénurie d'adresses. Plusieurs solutions ont été imaginées pour pallier la pénurie. Celle retenue, IPv6, porte l'espace d'adressage de 32 à 128 bits. La section 10.8 en expose les principes.

10.5 TRANSMISSION CONTROL PROTOCOL (TCP)

10.5.1 Généralités

TCP est un protocole de transport de bout en bout en mode connecté (figure 10.43). La numérotation des données diffère de celle du transport d'ISO. En effet, les compteurs d'ISO comptent des unités de données (N° séquence, N° attendu) alors que les compteurs de TCP pointent sur des octets (N° d'octet ou offset, N° d'octet attendu), ce qui fait dire que TCP transporte un flot d'octets. La longueur maximale de l'unité de données est de 64 ko.

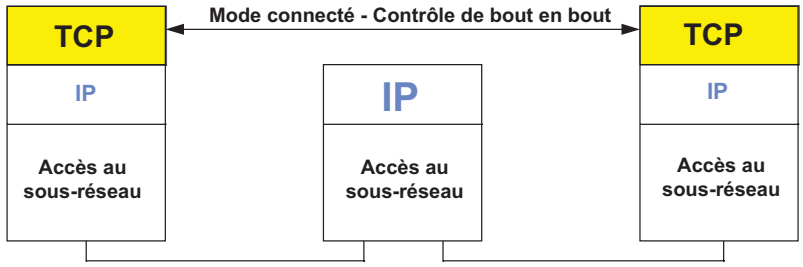


Figure 10.43 Transmission Protocol.

S'appuyant sur un protocole réseau non fiable (*best effort*), TCP doit assurer la délivrance en séquence des différents segments, contrôler la validité des données reçues, organiser les reprises sur erreur ou sur temporisation et réaliser le contrôle de flux.

10.5.2 Le message TCP et les mécanismes associés

Structure du segment TCP

TCP ne définit qu'un seul format de segment contre dix pour les messages de transport d'ISO. De ce fait, l'en-tête de TCP est prévu à la fois pour le transport des données, des ACK et des commandes (figure 10.44).

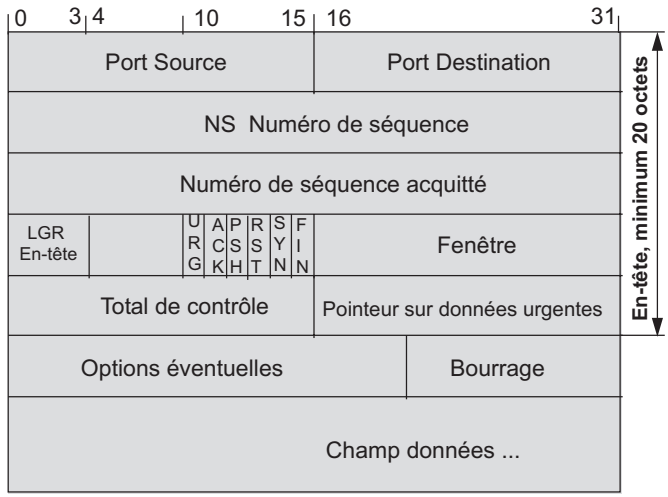


Figure 10.44 Structure de la TPDU ou segment TCP.

© Dunod – La photocopie non autorisée est un délit

Les différents champs du segment sont :

– Numéro de port (2 fois 16 bits), valeurs spécifiées à la connexion, et identifiant celle-ci. Le port destinataire est soit connu, soit défini lors d'une phase d'identification (login) et passé à l'appelant en réponse.

– Numéro de séquence sur 32 bits, une valeur initiale et aléatoire (**ISN**, numéro de séquence initial) est définie et acquittée par les deux systèmes d'extrémité lors de la phase de connexion. Le numéro de séquence indique le rang du premier octet du segment transmis, les octets sont décomptés depuis le début de la connexion (Ns = ISN + Nb octets transmis + 1). Le numéro de séquence du premier octet transmis est (ISN +1).

– Le numéro de séquence acquitté indique le numéro du prochain octet attendu, c'est-à-dire le numéro de séquence du dernier segment reçu, incrémenté de la taille des données reçues.

– Longueur de l'en-tête ou *offset* (4 bits) indique la longueur de l'en-tête du segment TCP en multiples de 4 octets. La valeur 5 correspond à taille minimale de l'en-tête TCP (20 octets). Le champ longueur d'en-tête pointe sur le début des données.

– Un espace de 6 bits est disponible.

– Le champ drapeau contient 6 indicateurs[10] :
  – **URG** valide le champ pointeur sur données urgentes.
  – **ACK**, le bit ACK à 1 valide le champ numéro de séquence acquitté.
  – **PSH**, TCP peut, pour des raisons d'efficacité du protocole, attendre d'avoir suffisamment de données à transmettre pour former un segment. L'indicateur PUSH permet de demander au destinataire de délivrer immédiatement les données en attente. Par exemple, l'application terminal virtuel associe, au caractère retour chariot (CR), la commande PSH.
  – **RST**, suite à la détection d'une anomalie grave sur le réseau, RST demande au destinataire de réinitialiser la connexion.
  – **SYN**, à 1 ce bit correspond à une demande de connexion, cet indicateur valide l'échange et l'acquittement des numéros de séquence initiaux (ISN).
  – **FIN**, ce drapeau correspond à une demande de déconnexion émise par l'un des interlocuteurs. Le destinataire d'une demande de déconnexion n'est pas obligé de s'exécuter (rupture de connexion négociée).

– Le champ fenêtre (2 octets) indique, en octets, la valeur de la fenêtre en réception, cette valeur varie dynamiquement en fonction de l'état du récepteur.

– Le total de contrôle est calculé sur l'ensemble du segment TCP, en-tête compris.

– Le pointeur sur données urgentes pointe sur le dernier octet urgent du champ de données. Dans TCP, il n'y a pas de notion de données express, les données comprises entre le début du champ données et la valeur du pointeur données urgentes sont traitées, en priorité, par le destinataire.

10. Un segment TCP où les bits SYN, URG, PSH et FIN sont à 1 et qui ne contient qu'un octet de données est nommé « paquet Kamikaze ».

Gestion de la connexion de transport et de l'échange

➤ Référence de transport et socket

TCP est un protocole de transport fiable, il établit, entre les processus communicants, une connexion. La connexion de transport TCP peut être comparée à la session ISO. Un même système peut établir plusieurs connexions de transport (multiplexage des connexions de transport). Afin de distinguer les différents flux, l'entité de transport référence ceux-ci (référence de transport). Une référence de transport définit complètement une connexion par l'association de différents identifiants (figure 10.45) :

– l'identifiant des processus d'extrémité ou port,

– l'identifiant des systèmes d'extrémité ou adresses IP,

– l'identifiant du protocole de transport utilisé.

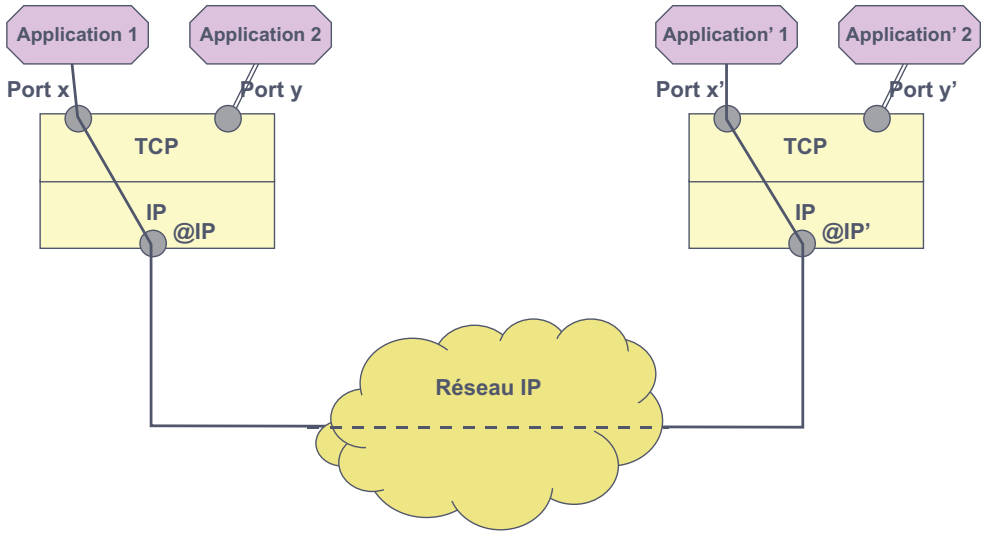


Figure 10.45 Connexion de Transport.

L'association : {**protocole, port destination, @IP destination, port source, @IP source**} est désignée sous le terme de *socke*t (RFC 793). La notion de socket est cependant beaucoup plus large. Une socket définit une interface de programmation ou **API**, *Application Programming Interface*, dans le monde UNIX. L'environnement Microsoft définit un concept identique : les WinSock.

➤ Notions de port

Un port identifie un ou plusieurs processus. La notion de port autorise le multiplexage des connexions sur une même machine (figure 10.46).

C'est la couche transport qui attribue, un numéro de port, à une connexion... Les 1 024 premiers ports sont réservés, ils sont dits **référencés**[11] (*Well known ports*).

11. Les ports référencés par la RFC 1060 et les ports référencés localement pour les applicatifs privés sont décrits, sous Unix, dans le fichier \etc\services.

© Dunod – La photocopie non autorisée est un délit

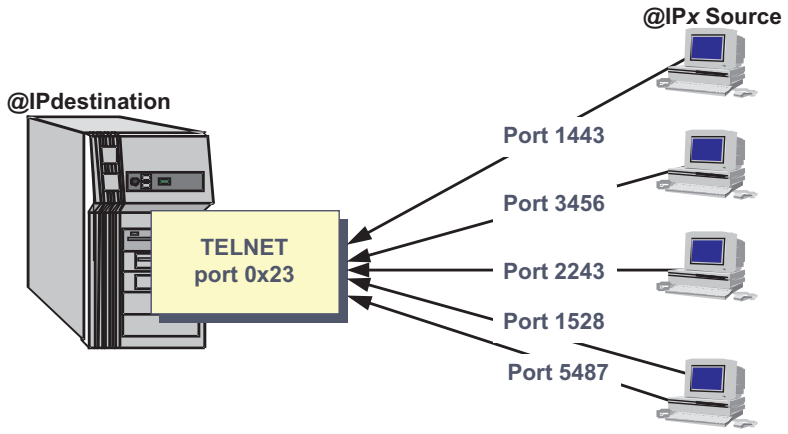


Figure 10.46 Multiplexage des connexions de transport.

Le tableau de la figure 10.47 contient quelques exemples de numéro de port tels qu'ils sont décrits dans la RFC 1060 (*Assigned Numbers*).

Nom du service	Numéro de port/Protocole	Alias	Commentaire
echo	7/tcp		
ftp-data	20/tcp		Protocole de transfert de fichiers
ftp	21/tcp		
telnet	23/tcp		Emulation de terminal
domain	53/udp	nameserveur	Serveur de noms de domaine
x400	104/tcp		Courrier ISO
pop3	110/tcp	postoffice	Bureau de poste
nbsession	139/tcp	netbios_ssn	Session de service Netbios

Figure 10.47 Exemples de numéros de ports référencés.

Les ports référencés permettent à une application dite cliente d'identifier une application sur un système distant. L'extrémité de la connexion cliente est identifiée par un numéro de port attribué dynamiquement par le processus appelant (figure 10.48). Ce numéro de port est dit port dynamique ou éphémère. Dans la figure 10.48, le port 23 est un port référencé, le port xxxx est un port éphémère permettant l'identification distante du flux de données.

Figure 10.48 Le référencement de la connexion de transport.

➤ Établissement de la connexion de transport

L'ouverture de connexion de TCP est très similaire à celle de TP4 ISO, c'est une ouverture avec validation en trois phases. Cependant, TCP définit deux modes d'ouverture : un mode passif et un mode actif. Dans le mode passif, TCP est en attente d'une demande d'ouverture en provenance d'un autre système (défini ou non). Dans le mode actif, TCP adresse une demande de connexion à un autre système identifié (figure 10.49).

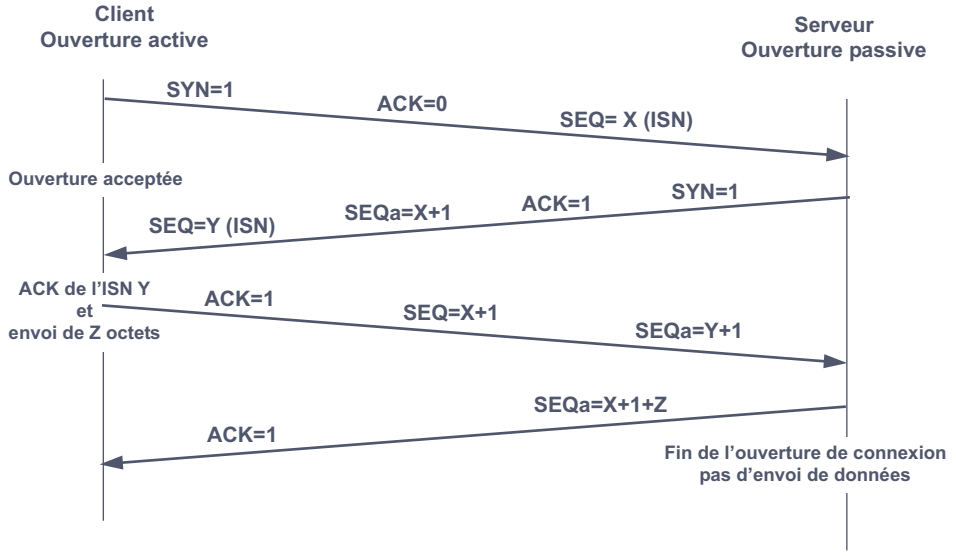


Figure 10.49 Ouverture d'une connexion en trois temps[13].

Ce sont les bits SYN et FIN qui indiquent respectivement une demande d'ouverture de connexion et de rupture de connexion. Le client émet une requête de connexion avec le bit SYN positionné à 1. Si le destinataire (le serveur) accepte cette connexion, il y répond avec un message dans lequel les bits SYN et ACK sont positionnés à 1. La connexion n'est ouverte que lorsque le demandeur acquitte ce dernier message (connexion en trois temps).

➤ Contrôle de l'échange

À l'instar d'autres protocoles, pour fiabiliser la connexion et de détecter d'éventuels segments perdus, TCP numérote les octets transmis (numéros de séquence sur 32 bits) et il identifie la position (*offset*), dans le flux de données, du premier octet du segment transmis.

TCP peut, sur un même couple de ports, accepter une connexion après fermeture de la précédente. Des données appartenant à l'ancienne connexion et retardées dans le réseau peuvent alors être prises en compte sur la nouvelle connexion. Pour différencier les connexions, TCP attribue à chaque connexion un numéro de séquence initial (**ISN**, *Initial Sequence Number*) différent. Le décomptage des octets transmis ne démarre pas à 0, mais à une valeur initialisée

13. Le sigle « SEQa » de la figure 10.50 désigne le champ N° de séquence acquitté.

© Dunod – La photocopie non autorisée est un délit

à partir d'une horloge interne[14]. La probabilité pour que le numéro de séquence du segment retardé de la précédente connexion corresponde au numéro de séquence attendu de la nouvelle connexion est très faible.

Lors de la connexion (figure 10.50), chaque extrémité informe l'autre du numéro de séquence initial choisit (ISN), ce qui conduit à un processus de connexion en trois temps :

– à la demande de connexion l'initiateur informe son destinataire de ISN choisi ;
– le destinataire l'acquitte et fournit son ISN ;
– en réponse l'initiateur l'acquitte ; durant cette dernière phase il est possible d'envoyer des données. Dans l'ouverture de connexion représentée figure 10.49, le serveur n'ayant aucunes données à envoyer, accepte seulement la connexion.

Un segment TCP peut contenir des données et transporter l'ack d'un segment reçu. Cette technique est connue sous le nom de **superposition de données** (*piggybacking*). TCP acquitte un octet dans le segment, l'acquittement est cumulatif, c'est-à-dire que l'octet acquitté acquitte tous les octets précédemment envoyés. Cette technique évite les retransmissions sur acquittement perdu.

➤ Fermeture de la connexion

La fermeture de connexion est aussi similaire à celle de l'ISO, mais il existe un mode de fermeture douce ou négociée évitant toute perte de données dans le réseau (il n'y a pas de couche session pour contrôler le dialogue). La fermeture définitive n'ayant lieu qu'après le transport effectif des données en attente dans les deux systèmes d'extrémité.

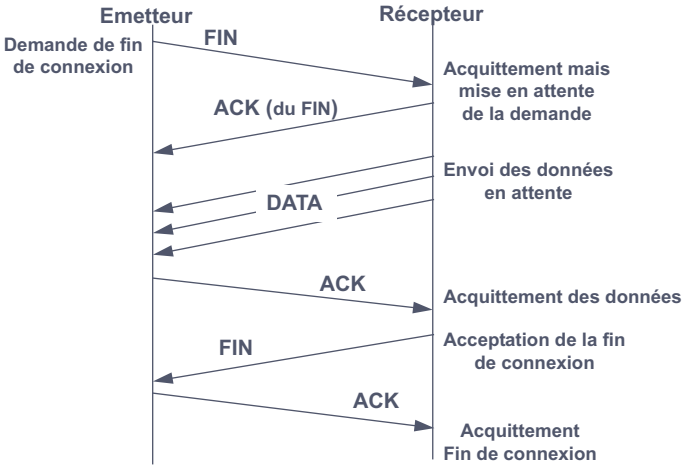


Figure 10.50 Fermeture négociée de TCP.

La figure 10.50 montre le mécanisme de fermeture douce. Lors de la demande de déconnexion de A (bit Fin = 1), si B a encore des données à envoyer, il procède à leur émission, puis accepte la déconnexion (Fin = 1). Celle-ci est acceptée par A, la connexion est fermée.

14. Ce mécanisme a les mêmes objectifs que le gel de référence de TP4 d'ISO. Le compteur d'initialisation est incrémenté toutes les 4 microsecondes, un même ISN est donc tiré toutes les 4 heures 30 environ.

Contrôle de flux et de congestion

➤ Contrôle de flux

Le contrôle de flux est traité de manière analogue à celui de la couche transport d'ISO. Il s'agit d'un mécanisme à fenêtre dynamique ou contrôle de flux explicite. Le crédit accordé est un crédit en octets et non pas en T_PDU comme TP4 d'ISO. Ce mécanisme peut conduire à un blocage des systèmes en cas de réduction de la fenêtre, par le destinataire, et de déséquencement dans l'arrivée des informations d'évolution de la fenêtre. TP4 d'ISO résout ce problème par la sous-numérotation des ACK, TCP n'apporte aucune solution à ce problème.

Dans la figure 10.51, le buffer du récepteur est plein, il ne peut plus accepter de données. Il en informe l'émetteur en positionnant le champ fenêtre à 0. L'émetteur cesse ses émissions. Cependant pour maintenir l'état actif de la connexion, l'émetteur sollicite périodiquement le récepteur en lui envoyant 1 octet de données. Le récepteur ne pouvant accepter les données, les ignore, et continue de signaler une valeur de la fenêtre toujours à zéro. Le processus se poursuit jusqu'à ce que le récepteur débloque la situation en ouvrant la fenêtre.

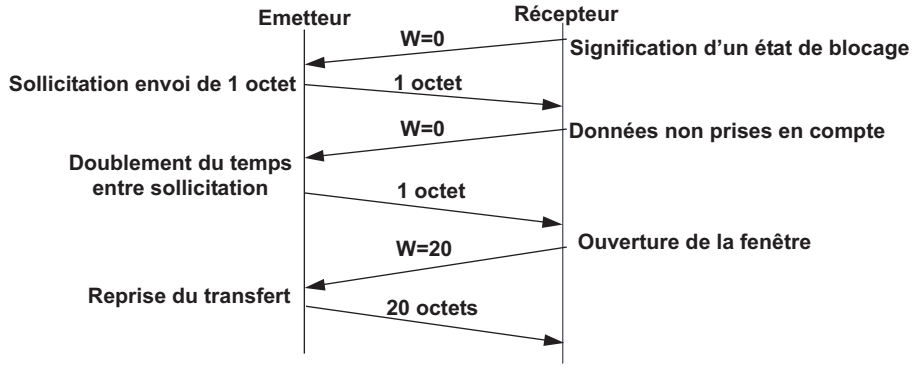


Figure 10.51 Principe du contrôle de flux par TCP.

➤ Notion de fenêtre stupide (*Silly Window Syndrome, SWS*)

Supposons que le buffer du récepteur se vide lentement. Il va ouvrir la fenêtre d'une petite quantité, l'émetteur va alors immédiatement envoyer des données. La fenêtre se referme. L'équilibre ne sera trouvé que par l'envoi de petits segments. Le réseau est alors mal utilisé. Plusieurs mécanismes, côté émetteur et récepteur, peuvent être utilisés pour éviter ce phénomène. Notamment le récepteur ne peut rouvrir la fenêtre que lorsque celle-ci a atteint la valeur minimale entre :

– la taille maximale du segment négocié (MSS),
– la moitié de la mémoire allouée à la connexion.

Du côté émetteur, il suffit de mémoriser les données pour éviter l'envoi de petits segments (groupage).

➤ Contrôle de la congestion

Le mécanisme décrit ci-dessus concerne l'asservissement de la cadence d'émission sur les capacités de réception du destinataire ; il s'agit d'une technique de contrôle de flux. Aucun mécanisme spécifique dans le réseau ne veille au contrôle de congestion (*best effort*). TCP

© Dunod – La photocopie non autorisée est un délit

implémente un mécanisme de gestion de la congestion spécifique, puisque ce sont les entités de bout en bout qui remédient à un problème interne au réseau. En cas de congestion, les ACK sont retardés et les données réémises, ce qui contribue à renforcer la congestion. Pour y remédier, à chaque segment perdu, le TCP émetteur réduit ses émissions (gestion d'une fenêtre de congestion) par réduction dichotomique de la fenêtre d'émission et, pour ne pas surcharger de réseau de retransmission peut-être inutilement, il augmente la valeur du timer de retransmission. En effet, l'ACK peut simplement avoir été retardé par l'état de congestion naissante.

Le contrôle d'erreur

TCP et UDP utilisent tous les deux la même technique de contrôle d'erreur. Deux objectifs sont assignés au total de contrôle :

– s'assurer que les données transmises n'ont pas été altérées durant le transfert ;

– garantir que les données sont délivrées au bon destinataire.

À cet effet, TCP utilise une technique particulière. Pour le calcul, il adjoint au segment TCP (ou UDP) un pseudo en-tête contenant, notamment, les adresses IP source et destination. L'inclusion de ces adresses dans l'en-tête de contrôle permet de protéger celles-ci par le total de contrôle. Le calcul du total de contrôle porte sur les données, l'en-tête TCP (ou UDP) et le pseudo en-tête IP (figure 10.52). Le récepteur effectue le calcul de la même manière, il reconstitue le pseudo en-tête à l'aide de sa propre adresse IP et des informations extraites de l'en-tête IP du datagramme reçu (adresse IP...). Cette manière de procéder garantit l'intégrité des données et la délivrance au bon destinataire, mais est en violation avec la règle d'indépendance des couches.

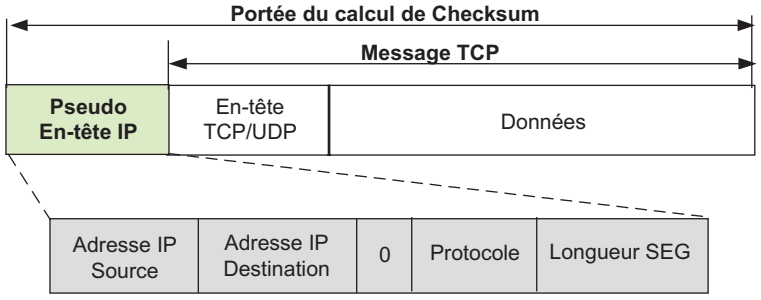


Figure 10.52 Portée du contrôle d'erreur dans UDP et TCP.

Le mode de calcul est identique à celui mis en œuvre par IP. Il s'agit du complément à 1 de la somme en complément à 1 des mots de 16 bits du segment TCP (UDP), pseudo en-tête inclus. Le pseudo en-tête n'est pas transmis, il est reconstitué par le destinataire. Dans le datagramme IP, seul l'en-tête est protégé par un total de contrôle.

La « bufferisation » des données

Pour optimiser la transmission, TCP attend, avant de transmettre des données, que le buffer d'émission soit plein (réduction des *overhead*). Cette technique est dénommée groupage ou (*clumping*). Certaines applications, notamment les applications de type terminal virtuel, peuvent exiger la transmission immédiate. Le positionnement du bit PUSH oblige TCP à délivrer les données immédiatement. Le mécanisme du *clumping* est illustré figure 10.53.

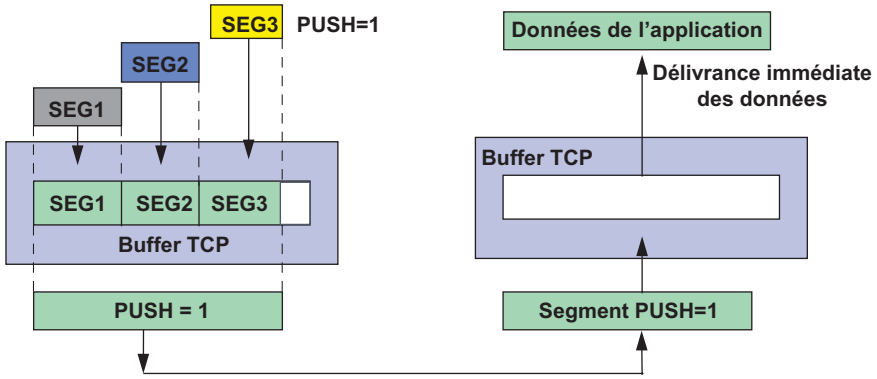


Figure 10.53 Fonction du bit PUSH.

Le bit PUSH est positionné à la fin de chaque séquence Commande/Réponse d'une application interactive et lors du dernier bloc d'un transfert de fichier sous FTP.

Le mode datagramme (UDP)

Certaines applications, notamment les applications temps réel nécessitent des temps de traitement optimisés, d'autres n'ont que très peu de données à envoyer, comme, par exemple le service de noms (DNS), d'autres encore n'ont nullement besoin d'un service sécurisé comme l'offre TCP, comme les informations de gestion des réseaux (SNMP). Dans tous ces cas les mécanismes mis en œuvre par TCP s'avèrent lourds et pénalisent les performances. Aussi, un mode de transport allégé a-t-il été défini, ce mode est appelé **UDP** (*User Datagram Protocol*).

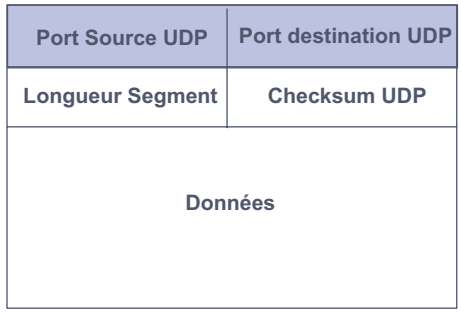


Figure 10.54 Format du segment UDP.

Le segment (datagramme) UDP ne contient que les champs ports source et destination (2 fois 2 octets, les valeurs attribuées sont différentes de celles de TCP), le champ longueur totale du datagramme (en-tête compris sur 2 octets), le champ total de contrôle (2 octets) et les données utilisateurs (figure 10.54). L'utilisation du champ checksum est facultative, dans ce cas, le champ est à 0.

Conclusion

La pile protocolaire TCP/IP offre deux modes de transport, un mode assuré, TCP, qui garantit la délivrance de données, le contrôle de flux et de congestion, et un mode allégé, UDP, gage de performance mais sans garantie de délivrance.

© Dunod – La photocopie non autorisée est un délit

10.6 LES PROTOCOLES DE LIAISON (POINT À POINT)

10.6.1 Généralités

Bien que défini à l'origine pour s'appuyer sur des réseaux physiques existants, très vite la nécessité de définir des protocoles de niveau 2 est apparue (figure 10.55).

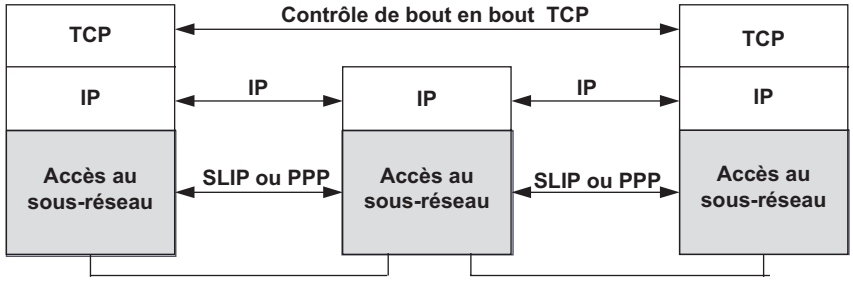


Figure 10.55 Position des protocoles de liaison.

Les paquets IP ne peuvent être émis directement sur une liaison série. En effet, il convient au minimum d'assurer la délimitation du bloc de données (datagramme), c'est l'un des rôles essentiels des protocoles de liaison (10.56).

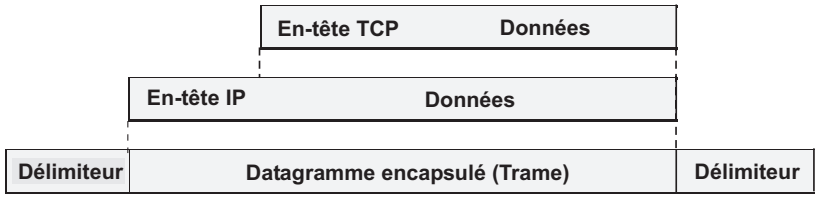


Figure 10.56 Délimitation des blocs de données.

Deux protocoles de liaison ont été spécifiés : **SLIP** (*Serial Line IP*) et **PPP** (*Point-to-Point Protocol*), le premier n'est utilisé que dans des liaisons point à point locales, car il suppose une ligne fiable, le second est notamment utilisé pour accéder, à travers le réseau téléphonique, à Internet.

10.6.2 SLIP, Serial Line Internet Protocol (RFC 1055)

SLIP est un protocole asynchrone orienté bloc. Très simple, il n'effectue que la délimitation de trames, et n'offre aucun mécanisme de détection et de reprise sur erreur (figure 10.57). Seule, la transparence aux caractères de délimitation est réalisée.

END 0xC0	Caractères à transmettre	END 0xC0

Figure 10.57 Format de la trame SLIP.

Le caractère END (192 ou 0xC0) est utilisé comme délimiteur de début et de fin. La transparence de caractère (un caractère END dans le champ données ne doit pas être interprété comme

un délimiteur) est assurée par le remplacement du caractère END par la séquence ESC_SLIP[15], ESC_END (0xDB, 0xDC). Le caractère d'échappement (ESC_SLIP) est lui-même protégé par l'insertion de la séquence ESC_SLIP, ESC_ESC (0xDB, 0xDD).

Rappelons, que dans un protocole asynchrone chaque caractère est précédé d'un bit de Start et suivi par un bit de Stop. La liaison SLIP est considérée comme un sous-réseau IP, de ce fait chaque extrémité possède une adresse IP (adresse de LS).

10.6.3 PPP, Point to Point Protocol (RFC 1548)

Afin de pouvoir, sur une même liaison, transporter des blocs d'information issus de protocoles de niveau supérieur différents (c'est le cas par exemple d'une liaison entre deux routeurs multiprotocoles), il est nécessaire d'introduire, dans le bloc de données, un champ identifiant le protocole transporté.

PPP est un protocole de liaison point à point inspiré d'HDLC. Le format et la signification des champs de la trame sont similaires à ceux d'HDLC. Seul, un champ protocole, sur deux octets, a été ajouté.

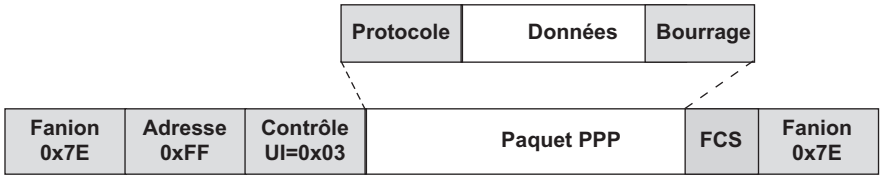


Figure 10.58 Format de la trame PPP.

L'une des particularités de PPP c'est d'avoir été prévu pour fonctionner aussi bien sur une liaison asynchrone que sur une liaison synchrone.

Si le protocole est utilisé sur une liaison synchrone, la transparence au fanion est assurée de manière similaire à HDLC (insertion d'un bit à 0 tous les 5 bits à 1, technique dite du *bit stuffing*). S'il est utilisé sur une liaison asynchrone la transparence au fanion (0x7E) est utilisée par remplacement de ce caractère par la séquence : ESC_PPP, ESC_FLAG (0x7D, 0x5E). Le caractère d'échappement (ESC_PPP, 0x7D) est remplacé par la séquence : ESC_PPP, ESC_ESC (0x7D, 0x5D).

Pour éviter que certains caractères (valeur ASCII inférieure à 32) ne soient considérés par les modems comme une commande, ils sont remplacés par des séquences de caractères spécifiques. Les caractères dont la transparence doit être assurée sont négociés à la connexion (table **ACCM**, *Asynchronous Control Character Map*). La transparence de ces caractères est obtenue par la séquence ESC_PPP, ESC_Commande où la valeur de ESC_Commande est la valeur ASCII de la commande avec le sixième bit complémenté (inversé).

Hors le champ données qui encapsule le datagramme IP, les différents champs de la trame PPP sont (figure 10.58) :

– Le champ adresse**,** inutile sur une liaison point à point, sa valeur est constante et fixée à 0xFF.

15. Le caractère d'échappement utilisé par le protocole SLIP est différent du caractère d'échappement du code ASCII. Pour le distinguer, nous le noterons ESC_SLIP, de même celui utilisé par le protocole PPP sera noté ESC_PPP.

© Dunod – La photocopie non autorisée est un délit

– Le champ commande a la même signification qu'en HDLC. Si la liaison est fiable et qu'aucun besoin de contrôle de séquencement n'est utile (fenêtrage) sa valeur est fixée à 0x03 (trame UI). En cas d'utilisation du format UI (trame d'information non numérotée), les champs adresse et commande sont inutiles, ils peuvent être omis dans les trames émises (négociation à la connexion).
– Le champ protocole, sur 2 octets, identifie le protocole de niveau supérieur. Il peut, lors de la connexion, être négocié sur 1 octet. Le tableau de la figure 10.59 donne, en exemple, quelques valeurs du champ protocole.
– Le champ FCS dont le mode de calcul est identique à celui de HDLC.

Valeur	Protocole
0x0021	IP
0x002B	IPX
0x002D	TCP/IP (en-tête compressé)
0x800F	IPV6

Figure 10.59 Exemple de valeurs du champ protocole.

PPP comprend un ensemble de sous-protocoles qui autorisent la négociation de paramètres et la sécurisation des échanges. Lors de l'initialisation d'un transfert, PPP entame une procédure de négociation des paramètres de l'échange par l'intermédiaire du protocole **LCP** (*Link Control Protocol*). Le protocole **PAP** (*PPP Authentification Protocol*) permet l'échange de mots de passe (en clair) avant le transfert de données. Alors que **CHAP** (*Challenge Authentification Protocol*), s'il est utilisé, effectue un contrôle tout au long de la communication par l'échange de « sceaux » cryptés (clé publique, clé secrète). Le protocole **NCP** (*Network Control Protocol*) permet la négociation de paramètres du niveau réseau (affectation d'adresses IP, compression d'en-tête)

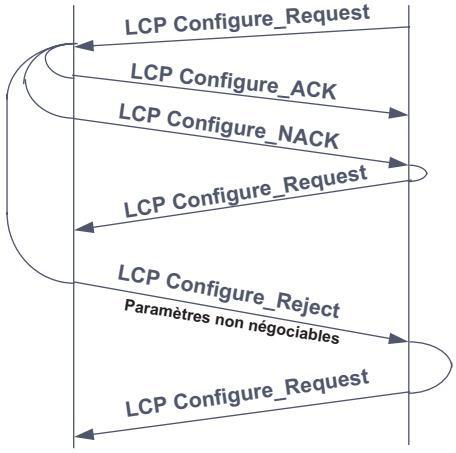


Figure 10.60 Phases d'initialisation de PPP.

Le protocole NCP, *Network Control Protocol*, permet, dès l'établissement de la liaison, de négocier certains paramètres de connexion. Chaque extrémité négocie ses propres options (figure 10.60). Les paramètres proposés peuvent être acceptés (ACK), refusés (NACK) ; ils seront, dans ce dernier cas, renégociés. Ils peuvent aussi être non négociables (Reject), dans

ce cas l'extrémité réitère une phase de négociation avec comme paramètres et valeurs ceux contenus dans la trame Reject.

La liste des paramètres négociables est codée selon le format : Type, Longueur, Valeurs. Exemples de paramètres négociables :

– **MRU** (*Maximum Receive Unit*) correspond à la longueur de la trame (trame de longueur fixe). Par défaut cette valeur est fixée à 1 500 octets. Si l'unité de données à envoyer est de taille inférieure au MRU négocié à la connexion, des données de bourrage seront insérées ;

– **ACCM** (*Asynchronous Control Character Map*) cette table assure la transparence des caractères de commande. Les caractères concernés sont les 32 premiers caractères de la table ASCII. À chaque caractère correspond 1 bit de la table ACCM, le 5^{e} bit à 1 indique par exemple que le 5^{e} caractère sera transcodé (transparence). Chaque caractère indiqué sera codé, dans le champ données comme suit : caractère d'échappement (0x7D) + caractère transcodé (OU exclusif avec 0x20 : le sixième bit est positionné à 1)

10.7 EXEMPLES D'APPLICATIONS TCP/IP

10.7.1 Le service de noms (DNS)

Généralités

Rappelons que le nommage est une notion complémentaire de celle de l'adressage, l'un désigne l'objet (objet nommé) l'autre sa localisation[16]. Le **DNS** (*Domain Name System*) est une base de données distribuée s'appuyant sur UDP (Port 53).

D'origine **IAB** (*Internet Activities Board*), le DNS est une base de données distribuée basée sur le modèle relationnel client/serveur. La partie cliente, le solveur (*resolver*), est chargée de résoudre la correspondance entre le nom symbolique de l'objet et son adresse réseau. En introduisant un nommage hiérarchique et la notion de domaine (chaque nœud de la hiérarchie peut être un domaine ou sous-domaine de nommage), le DNS présente les avantages suivants :

– gestion simplifiée du nommage (nommage hiérarchique) ;

– délégation et répartition des responsabilités d'attribution de noms et d'administration par domaine de nommage ;

– duplication possible de la base (notion de serveur maître ou primaire et de serveur secondaire), le serveur secondaire pouvant répondre à une requête si le serveur principal est occupé. La mise à jour se fait uniquement sur le serveur maître avec réplication automatique des données modifiées sur le serveur secondaire ;

– indépendance vis-à-vis d'un constructeur, les resolvers DNS sont, en principe, disponibles sur tous les environnements TCP/IP.

L'espace de nommage

Les noms sont organisés selon une structure arborescente hiérarchique (arbre inversé) appelée **espace de nommage** (figure 10.62). La racine est au sommet, son nom de domaine est vide,

16. Dissociant l'objet de sa localisation géographique, certains désignent le nom sous le terme d'adresse logique. Or, le concept IP de réseau logique tend plutôt à réserver à l'adressage du réseau logique le terme d'adresse logique.

© Dunod – La photocopie non autorisée est un délit

elle est symbolisée par un point (•). Le nombre de niveaux est limité à 127. Un nom ne peut dépasser 255 caractères et chaque niveau est limité à 63 caractères. La RFC 1032 préconise de limiter à 12 caractères le nom attribué à chaque niveau (nœud). Il n'y a pas de distinction Minuscule/Majuscule. Des nœuds peuvent avoir des noms identiques s'ils sont dans des domaines différents.

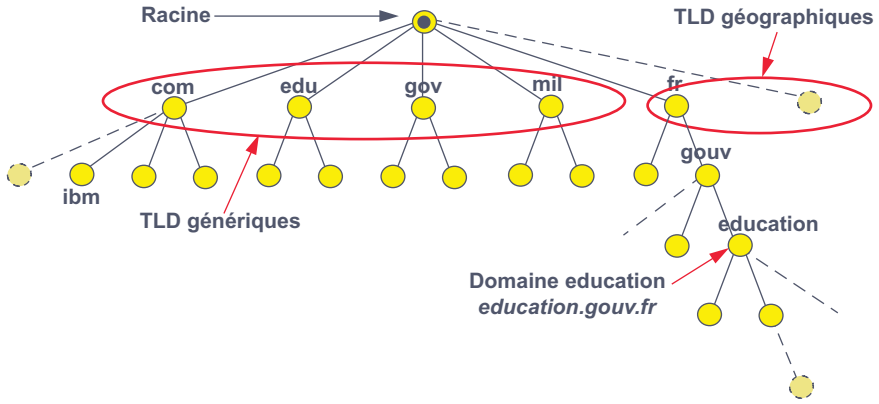


Figure 10.61 Structure de l'espace de nommage.

Dans la figure 10.61, le domaine éducation est un sous-domaine du domaine gouv. En principe, c'est l'IANA qui attribue les noms de domaine. Les noms de domaine géographique (TLD, Top Level Domain) sont, par délégation, attribués par des organismes régionaux, en France : l'AFNIC (domaine fr). Aucune signification n'est imposée aux noms de domaine sauf pour le premier niveau :

- **com**, organisations commerciales, en principe possédant des implantations sur plusieurs domaines géographiques (ibm.com) ;
- **edu**, établissements d'enseignement (réservé aux établissements des USA, mit.edu) ;
- **gov**, établissements gouvernementaux (USA, nsf.gov) ;
- **mil**, organisations militaires américaines (USA, army.mil) ;
- **net**, organisations du réseau Internet (bull.net) ;
- **org**, organisations non commerciales et non gouvernementales (ong.org) ;
- **int**, organisations internationales (onu.int) ;
- **arpa**, domaine réservé à la résolution de nom inversée ;
- organisations nationales dont la dénomination est limitée à 2 caractères (fr, uk, it...) ;
- ...

Une machine est désignée en indiquant l'arborescence complète de son nom (**FQDN**, *Fully Qualified Domain Name*).

La résolution de nom

➤ Principe

Le client DNS ou solveur (*resolver*) est un programme de type daemon. Sur sollicitation d'un programme demandeur, il est chargé d'émettre les demandes et de traduire les réponses. Lors

de la configuration d'une station IP, on lui fournit son nom de domaine, l'adresse de son serveur local de noms et, éventuellement, une liste ordonnée de serveurs de noms.

Le client solveur (figure 10.62) interroge le serveur de noms local. Si la recherche est infructueuse le serveur local interroge le serveur de niveau supérieur (recherche récursive) ou le client interroge lui-même d'autres serveurs (requête itérative).

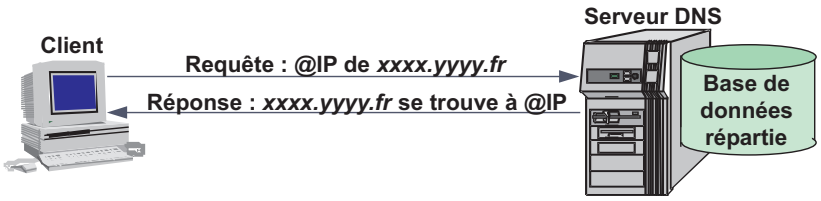


Figure 10.62 La résolution de nom.

➤ Fonctionnement du solveur

Lorsque le programme d'application formule une demande, le resolver interroge son cache (figure 10.63 gauche) : si la correspondance Nom/@IP y est déjà enregistrée, il fournit directement la réponse au programme demandeur.

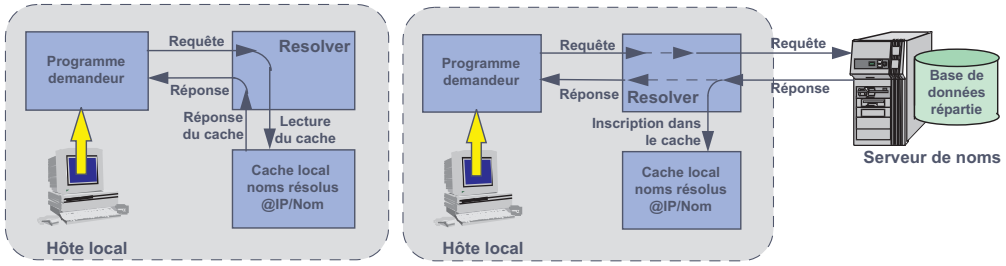


Figure 10.63 Fonctionnement du resolver.

Sinon, il émet une requête au serveur DNS. Celui-ci résout la demande, directement ou par requêtes itératives ou récursives. Le solveur analyse la réponse, met à jour son cache et fournit la réponse au demandeur (figure 10.63 droite).

➤ La résolution inverse

À l'instar de la résolution d'adresses (RARP), la résolution de noms inverse permet d'obtenir, à partir de l'adresse IP, le nom de la machine. Le domaine arpa, sous-domaine in-addr, a été prévu à cet effet (figure 10.64).

L'arbre inverse considère l'adresse comme un nom : par exemple l'adresse du Conservatoire National des Arts et Métiers (163.173.128.18) est traduite par 18.128.173.163.in-addr.arpa. À chaque octet de l'adresse IP correspond un nœud de l'arbre. Chaque sous-domaine ainsi défini comporte 256 sous-domaines. Le 4^{e} niveau correspond au nom du serveur connaissant le nom de domaine associé à cette adresse.

© Dunod – La photocopie non autorisée est un délit

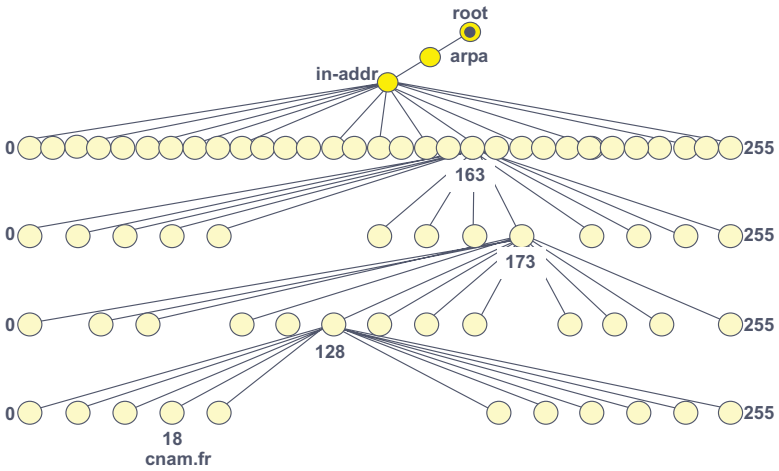


Figure 10.64 Arbre de résolution inverse.

10.7.2 Le transfert de fichiers

Le transfert de fichiers est l'une des applications les plus utilisées sur les réseaux. Le modèle TCP/IP en décline deux versions. L'une allégée (**TFTP**, *Trivial File Transfer Protocol*) nécessitant peu de mémoire et pouvant tenir en mémoire morte des machines sans disque (terminal X, par exemple) et permettre le téléchargement du système. TFTP utilise UDP. L'autre version, **FTP** (*File Transfer Protocol*) constitue un véritable système de manipulation de fichiers à distance.

TFTP (Trivial File Transfert Protocol)

TFTP permet le transfert de données en lecture (**RRQ**, *Read ReQuest*) ou en écriture (**WRQ**, *Write Request*) de fichiers en ASCII (mode dit netascii) ou en flux d'octets (mode dit octet). En mode ASCII, mode par défaut, le fichier est structuré en lignes, TFTP insère à la fin de chaque ligne les caractères CR/LF (*Carriage Return/Line Feed*, voir tableau des codes ASCII figure 2.5). Le transfert a lieu par bloc de 512 octets numérotés, la fin du transfert est détectée par un message de données de longueur inférieure à 512 octets (figure 10.65).

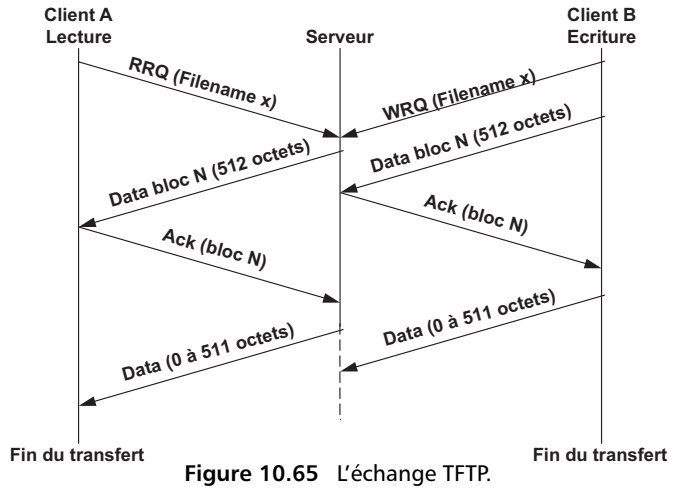


Figure 10.65 L'échange TFTP.

TFTP utilise UDP, c'est donc à lui de gérer les paquets perdus. Le protocole est du type *Send and Wait* (émettre et attendre), chaque extrémité gérant une reprise sur temporisation (transmission symétrique). Si ce procédé fiabilise la transmission, il peut provoquer une duplication des échanges. En effet (figure 10.66), supposons l'Ack du paquet N retardé, l'émetteur procède, sur temporisation, à la retransmission du paquet N. À réception de l'ACK de N l'émetteur envoie N + 1, qui sera acquitté, à la réception du second ACK de N, il renvoie encore N + 1, ces deux blocs seront acquittés...

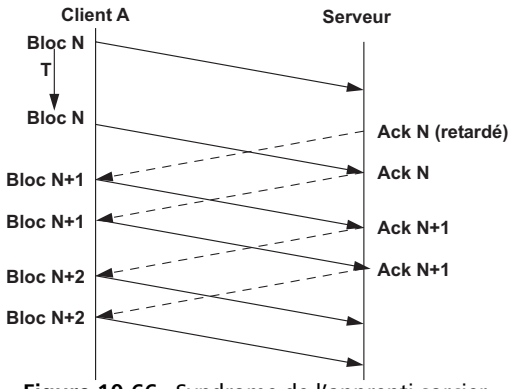


Figure 10.66 Syndrome de l'apprenti sorcier.

TFTP n'utilise que 5 types de messages décrits figure 10.67. Le nom de fichier, le mode et les messages d'erreur sont codés en ASCII. La fin de chaque libellé est indiquée par le code ASCII « 0 ». En principe, un message d'erreur peut se substituer à un Ack, une retransmission est alors réalisée. Cependant, dans la plupart des implémentations, un message d'erreur provoque l'arrêt du transfert.

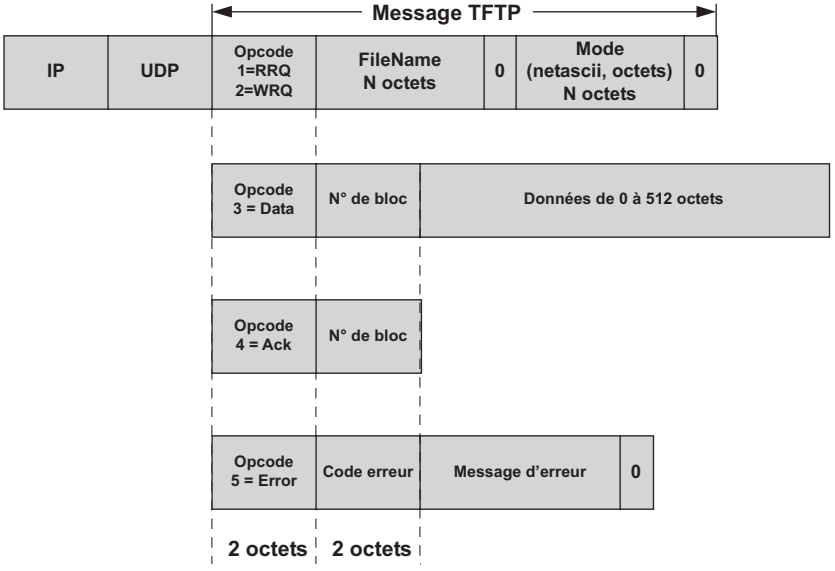


Figure 10.67 Format des messages TFTP.

Notons que TFTP attend les appels sur le port 69, or, contrairement à TCP, UDP ne gère pas le multiplexage des connexions sur un port. Pour remédier à cette lacune, TFTP attend

© Dunod – La photocopie non autorisée est un délit

les appels de connexions TFTP sur le port réservé 69 (messages RRQ ou WRQ) et répond sur un port éphémère que le client détectera dans la réponse (port source du message UDP de réponse).

FTP (File Transfert Protocol)

L'originalité de FTP est d'ouvrir pour chaque session FTP deux connexions simultanées. L'une sur le port 21 (FTP), l'autre sur le port 20 (FTP_Data). La première connexion, connexion de contrôle ou de service, sert à l'échange des messages FTP (connexion de signalisation), l'autre au transfert de données (figure 10.68). La demande de connexion FTP est établie sur le port 21 et reste active durant toute la session FTP (connexion permanente). La connexion de transfert sur le port 20 n'est active que durant le transfert effectif d'un fichier (connexion temporaire).

FTP permet de spécifier :

– le type de fichiers (ASCII, binaire, EBCDIC) ;

– la structure du fichier (par défaut flux d'octets) ;

– le mode de transmission (flux d'octets – valeur par défaut – ou mode bloc).

Contrairement à TFTP, FTP réalise un contrôle d'accès avant l'acceptation de toute connexion. En principe, il faut posséder un compte sur le serveur FTP pour pouvoir s'y connecter. La session FTP commence par une procédure de « *login* » : nom d'utilisateur, mot de passe. Il est aussi possible de se connecter sans compte (invité). Dans ce cas le nom d'utilisateur est *anonymous* et le mot de passe *guest* (connexion FTP anonyme). Généralement, lorsqu'un serveur admet les connexions anonymes, en principe l'accès est limité par l'administrateur à un seul répertoire dit répertoire public.

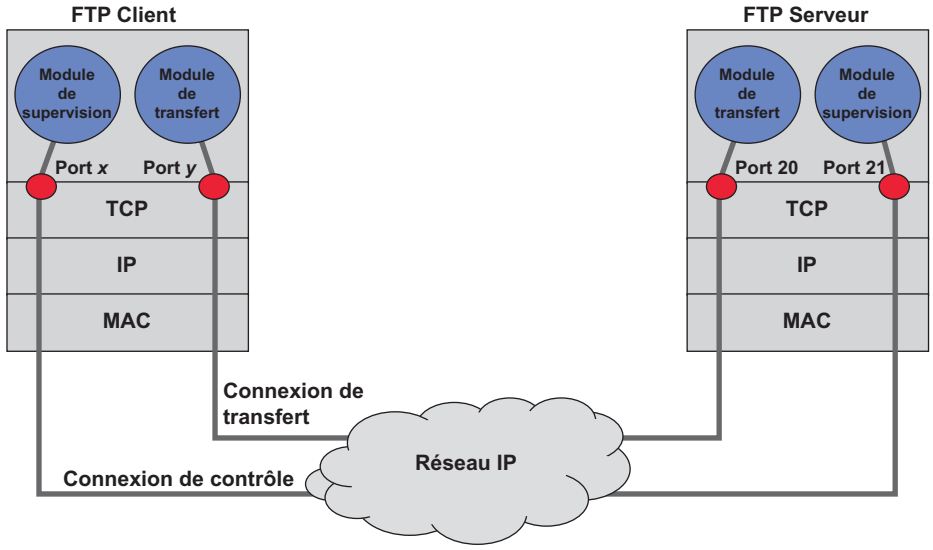


Figure 10.68 Les deux connexions de FTP.

Le tableau de la figure 10.69 fournit, à titre d'exemple, les commandes les plus courantes de FTP. La commande HELP liste l'ensemble des commandes disponibles sur un serveur.

Commande	Description
FTP	Invocation du service FTP, la phase de login suit.
USER nom-utilisateur	Spécifie le nom de l'utilisateur
PASS mot-de-passe	Mot de passe du compte utilisateur
CWD nom-de-chemin	Spécifie un répertoire de travail sur le serveur FTP
PORT hôte-port	Indique au serveur une adresse IP (hôte) et un numéro de port.
RETR nom-de-fichier	Indique au serveur le nom du fichier à transférer (get)
STOR nom-de-fichier	Indique au serveur le nom du fichier à recevoir (put)
DELE nom-de-fichier	Demande au serveur d'effacer nom-de-fichier
RMD nom-de-chemin	Suppression d'un répertoire sur le serveur
MKD nom-de-chemin	Création d'un nouveau répertoire sur le serveur
PWD	Demande au serveur de retourner le nom du répertoire courant
LIST nom-de-chemin	Liste tous les fichiers du répertoire nom-de-répertoire
ABOR	Arrête toutes les commandes en cours et ferme les connexions
QUIT	Termine la session et ferme la connexion de contrôle.

Figure 10.69 Listes des commandes usuelles de FTP.

10.7.3 L'émulation de terminal (TELNET)

Principe de Telnet

Le terminal virtuel est un logiciel en mode client/serveur. Le terminal serveur émule vis-à-vis d'un applicatif sur la machine serveur un terminal local avec lequel l'application échange des messages tandis que sur une machine distante, cliente de l'application, un terminal client est émulé sur un terminal physique. L'échange se fait en deux temps. Le premier a lieu entre le terminal client réel et le terminal serveur virtuel, le second entre le terminal serveur virtuel et l'application. Cette approche est illustrée figure 10.70.

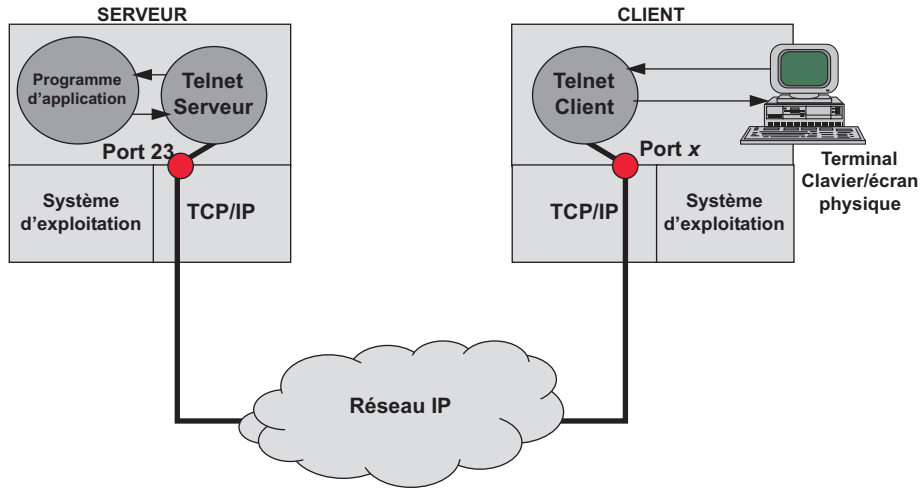


Figure 10.70 Principe du terminal virtuel.

© Dunod – La photocopie non autorisée est un délit

Les systèmes client et serveur pouvant être tout à fait différents, le terminal virtuel (**NVT**, *Network Virtual Terminal*) définit une syntaxe d'échange : le code ASCII américain à 7 bits. Chaque entité doit, éventuellement, réaliser l'adaptation nécessaire vis-à-vis du système hôte. L'échange se réalisant par octet, le bit de poids fort est toujours positionné à 0, sauf pour la valeur 255 (0xFF) qui signale que les caractères qui suivent sont une séquence de commande (caractère **IAC**, *Interprest As Command*). Une option de Telnet autorise l'emploi de caractères sur 8 bits, dans ce cas, pour assurer la transparence du caractère IAC, le caractère 255, dans le champ données, est doublé.

Commandes et modes de fonctionnement

S'adressant à divers systèmes, Telnet doit être capable de s'adapter au mieux aux capacités de chacune des extrémités. Aussi, divers modes de fonctionnement sont possibles et de nombreuses options peuvent être négociées par chacune des entités communicantes (négociation symétrique).

La requête de négociation est un ensemble de trois caractères : < IAC, requête, option>. Les différentes requêtes et les réponses possibles sont :

- **WILL**, l'émetteur sollicite l'accord pour l'option qui suit, le récepteur accepte (DO) ou refuse (DONT) ;
- **DO**, l'émetteur demande au récepteur d'utiliser l'option, le récepteur accepte (WILL) ou refuse (WONT) l'utilisation de l'option qui suit ;
- **WONT**, l'émetteur invalide une option, le récepteur ne peut qu'accepter (DONT) ;
- **DONT**, l'émetteur demande au récepteur d'invalider une option, le récepteur ne peut qu'accepter (WONT).

Seuls, deux modes de fonctionnement de Telnet sont utilisés aujourd'hui, ce sont le mode ligne (LINEMODE) et le mode caractère (terminal asynchrone). Dans le premier mode le terminal assure lui-même la gestion de l'affichage, les échanges entre le serveur et le terminal utilise le mode bloc (ligne). Dans le second mode, c'est le serveur qui gère l'affichage (écho du caractère frappé). Par exemple, lors du lancement d'une application qui nécessite le mode caractère comme l'éditeur vi de UNIX :

- Le serveur envoie la suite : <IAC, WILL, ECHO>, ce qui correspond à demander au terminal de passer en mode écho de caractère (*Will Use Echo Data*).
- Le client signifie son accord par la commande : <IAC, DO, ECHO> (*Start Use Echo Data*).
- Lors de la sortie du programme en cours, le mode de fonctionnement précédent est restauré par la demande d'invalidation de l'option ECHO <IAC, WONT, ECHO>.

Les tableaux de la figure 10.71 fournissent la liste des principales commandes et des options Telnet.

Le terminal Telnet ne permet pas seulement de se connecter pour une session de travail sur une machine distante, il a longtemps été utilisé comme terminal de consultation de données sur différents serveurs (météo...). Avec le déploiement d'Internet, cette dernière utilisation est aujourd'hui obsolète.

Commande	Valeur dec.	Valeur Hex.	Signification
IAC	255	FF	Interpréter le caractère suivant comme une commande
DON'T *xx*	254	FE	Refus d'une option, le caractère suivant '*xx*' identifie l'option refusée
DO *xx*	253	FD	Acceptation de l'option '*xx*' (Start Use)
WON'T *xx*	252	FC	Acquittement négatif de l'option '*xx*'
WILL *xx*	251	FB	Acquittement positif de l'option '*xx*' (Will Use)
GA	249	F9	Continuer (Go Ahead)
EL	248	F8	Effacer une ligne (Erase Line)
EC	247	F7	Effacer un caractère (Erase Character)
AO	245	F5	Arrêter l'édition (Abort Ouput)
IP	244	F4	Interrompre le processus (Interrupt Process)
BRK	243	F3	Break
NOP	241	F1	Opération nulle (Non OPeration)
EOR	239	EF	Fin d'enregistrement (End of Record)

Commande	Valeur dec.	Valeur Hex.	Signification
Transmit Binaire	00	00	Transmission en mode 8 bits
Echo	01	01	Écho des données introduites au clavier (Echo Data)
Suppress go ahead	03	03	Passage en mode caractère
Linemode	34	22	Passage en mode ligne
Carriage Return	10	0A	Retour chariot, Positionne le curseur en début de ligne
Line Feed	13	10	Passage à la ligne suivante

Figure 10.71 Principales commandes et options Telnet.

10.8 D'IPv4 À IPv6

10.8.1 Les lacunes d'IPv4

IPng (*next generation*) ou IPv6 répond au besoin d'évolution de la communauté Internet et comble les faiblesses d'IPv4. La plus connue concerne l'espace d'adressage, IPv4 met en place un adressage à plat (Net_ID) ce qui a conduit à l'explosion des tables de routage (certains routeurs Internet ont plusieurs dizaines de milliers d'entrées dans leur table de routage). Le CIDR (voir section 10.2.2) a partiellement répondu à ce problème en faisant disparaître la notion de classe d'adresses, en autorisant l'agrégation d'adresses de réseaux contigus en un seul préfixe réseau et en organisant une affectation géographique des adresses. La seconde concerne la prévisible pénurie d'adresses, l'utilisation d'un adressage privé associé à la translation d'adresses (NAT) résout partiellement ce problème mais pénalise fortement les performances.

Enfin, l'arrivée de nouvelles applications comme le multimédia et le besoin de services sécurisés ont motivé l'étude d'un nouveau protocole permettant d'augmenter l'espace d'adressage tout en conservant les grands principes qui ont fait le succès du protocole IP.

Les principales caractéristiques d'IPv6 sont :

– adressage étendu (128 bits au lien de 32) ;
– en-tête simplifié autorisant un routage plus efficace ;

© Dunod – La photocopie non autorisée est un délit

– sécurité accrue en incluant des mécanismes d'authentification, de cryptographie et en garantissant l'intégrité des données ;
– implémentation d'un mécanisme de découverte du MTU optimal. La fragmentation n'est plus réalisée dans le réseau mais par le nœud source ;
– suppression du champ checksum, ce qui allège le travail des routeurs intermédiaires ;
– amélioration des aspects de diffusion (multicast) ;
– intégration de fonctions d'autoconfiguration et de renumérotation.

10.8.2 Le datagramme IPv6

Structure du datagramme

Plusieurs solutions ont été envisagées pour augmenter l'espace d'adressage, la solution retenue passe l'adressage de 32 bits à 128 bits (2^{128} adresses soit plusieurs millions d'adresses par mètre carré de surface terrestre - 6,65 10^{23} @/m^2 -). Pour améliorer le traitement des datagrammes dans les routeurs, la structure même du datagramme a été modifiée en supprimant notamment le champ option et les champs obsolètes. Par conséquent, l'en-tête du datagramme est de longueur constante (40 octets). L'augmentation de longueur étant largement compensée par le gain de traitement d'une structure d'en-tête figée. La figure 10.72 rapproche les datagrammes IPv4 et Ipv6. Les champs IPv4 qui n'ont aucune correspondance dans le datagramme IPv6 ont leur label grisé et en italique.

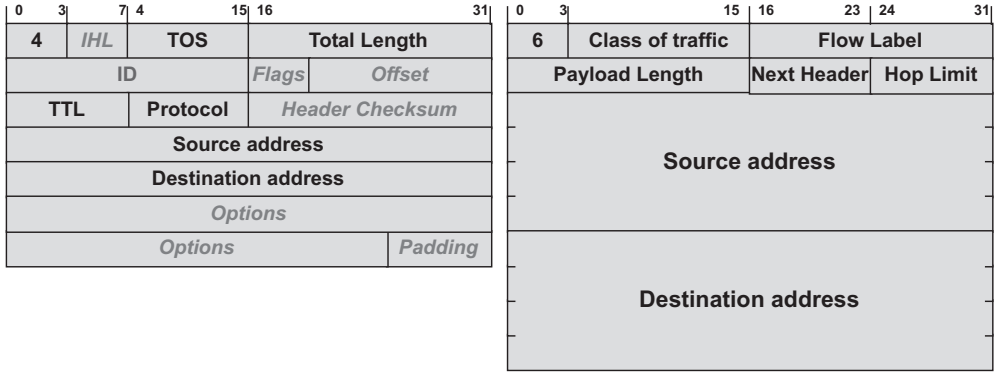


Figure 10.72 le datagramme IPv4 et IPv6.

Les données relatives à la fragmentation (ID, Flags, Offset) disparaissent de l'en-tête. IPv6 implémente un mécanisme de découverte de la MTU. La fragmentation est réalisée par la source et le réassemblage par le destinataire ce qui allège considérablement le travail des routeurs intermédiaires. Cependant, si la fragmentation s'avère indispensable une extension d'en-tête est prévue à cet effet. L'en-tête étant de longueur fixe, le champ IHL (longueur de l'en-tête) est devenu inutile. De même, le calcul du total de contrôle a été supprimé, le mécanisme de contrôle de TCP incluant un pseudo en-tête IP est suffisant pour protéger les adresses.

Le champ TOS trouve son équivalent en deux champs, un champ classe de trafic sur 8 bits et une identification de flux (*Flow Label*). Ce champ contient un identifiant attribué initialement

par la source, il est assimilable à un numéro de circuit virtuel. Le routage est ainsi plus efficace (commutation de niveau 3). Le contexte ainsi créé est détruit sur temporisation d'inactivité (*soft-state*[17]).

L'en-tête étant de longueur fixe, le champ longueur totale d'IPv4 (*Total length*) est remplacé par la taille des données transportées (*Payload Length*). Enfin, Le champ *protocol* d'IPv4 est transformé en indication sur le type de l'en-tête suivant (*Next Header*). Si aucune option n'est invoquée, ce champ contient l'identification du protocole transporté, le tableau de la figure 10.73 indique les différentes valeurs de ce champ. Enfin, un compteur de sauts (*Hops Limit*) positionné par la source (valeur par défaut 64) et décrémenté de 1 par chaque nœud intermédiaire remplace le champ TTL d'IPv4.

Valeur	Type	Désignation
0	Option	Hop-by-Hop
4	Protocole	IPv4
6	Protocole	TCP
17	Protocole	UDP
43	Option	Routing Header
44	Option	Fragment Header
45	Protocole	Interdomain Routing Protocol
46	Protocole	ReSsource reserVation Protocol
50	Option	Encapsulation Security Payload (IPsec)
51	Option	Authentification Header (Ipsec)
58	Protocole	ICMP
59		No Next Header
60	Option	Destination Options Header

Figure 10.73 Valeurs du champ Next Header.

Traitement des options ou en-têtes d'extension

➤ Généralités

Des extensions d'en-tête remplacent les options d'IPv4. Ces extensions sont ignorées des routeurs, seule l'extension Hop-by-Hop (Proche en Proche) est traitée par tous les routeurs. Afin de garantir des performances optimales, les options doivent apparaître dans un ordre prédéfini, l'extension Hop-by-Hop devant être la première. La figure 10.74 illustre le chaînage des en-têtes.

17. On peut classer les réseaux à états en deux catégories. Dans la première, le contexte est créé à l'initiative de l'appelant par un message spécifique et est détruit par un message de libération (notion de circuit virtuel). Ce type de réseau est aussi appelé *hard-state*. Dans les seconds, le contexte est déduit du flux de données, désignée sous le terme de *soft-state* par opposition au *hard-state*. Cette technique allège les réseaux, il n'y a pas de mécanisme explicite de création de circuit virtuel. Cependant, il n'y a aucune garantie de maintien du contexte durant toute la transmission.

© Dunod – La photocopie non autorisée est un délit

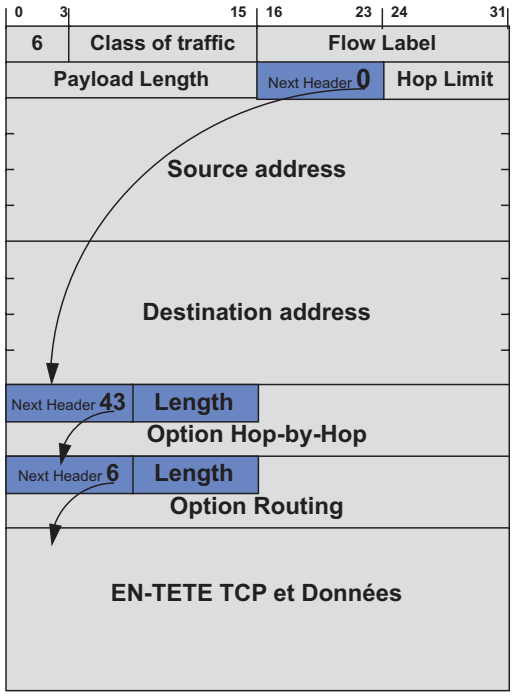


Figure 10.74 Principe du chaînage des options.

➤ Exemples d'extension d'en-tête

Extension Proche en Proche (0)

Cette extension, la première de la série, est la seule à être traitée par tous les routeurs traversés. La longueur de l'extension (champ length) est exprimée en mots de 64 bits-1. Cette extension est un champ d'option codé selon le triptyque classique <Type d'option, Longueur, Valeur>. Les différentes options définies sont :

– Des champs de bourrage, type 0 pour 1 octet de bourrage, type 1 pour une longueur de plus de 2 octets (alignement d'une extension sur un multiple entier de mots de 64 bits).

– *Router Alert* (type 5), utilisée pour indiquer au routeur qu'il doit examiner le contenu du champ données (messages ICMP ou RSVP).

– *Jumbogramme* (type 194), ce champ d'extension spécifie la longueur des données (valeur sur 4 octets) quand celle-ci dépasse 64 ko. Dans ce cas, le champ longueur des données de l'en-tête IPv6 contient la valeur 0.

Extension Routage (43)

Cette extension permet d'imposer une route à un paquet. Actuellement, seul le routage par la source est défini (type 0). Ce routage peut être soit strict, le routeur suivant doit alors être le voisin du routeur courant, soit libre (*loose*) le routeur peut consulter ses tables pour choisir la route à prendre pour joindre le routeur suivant de la liste. L'extension pour le routage par la source est une liste des routeurs à traverser.

Extension Fragmentation (44)

La fragmentation dans un réseau *best-effort* pénalise les performances. Même si IPv6 introduit un mécanisme de découverte de la MTU, certaines applications[18] considérant que le réseau assure la fragmentation remettent à la couche transport (UDP) des données trop importantes. Dans ces conditions, la couche IPv6 doit réaliser la fragmentation à l'émission, le réassemblage est réalisé par le destinataire. Le format de cette extension reprend les informations de segmentation d'IPv4 (figure 10.75)

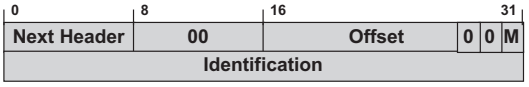


Figure 10.75 Format de l'extension fragmentation.

Les différents champs ont la même signification, à l'exception du bit DF inutile puisque la fragmentation n'est pas traitée par les routeurs traversés. Le bit M informe qu'un fragment suit. Le champ offset sur 13 bits indique en multiple de 8 octets, la position du premier bit du fragment dans le datagramme d'origine. Enfin, le champ identification, recopié dans tous les fragments d'un même paquet, permet l'identification par le destinataire de tous les fragments du paquet initial.

Extension Destination (60)

Codée de manière similaire à l'extension hop-by-hop, cette extension est traitée par le destinataire, elle introduit le concept de mobilité du destinataire. Un mobile pouvant toujours être joint par son adresse principale. Les options destinations permettent de gérer l'association entre une adresse locale sur le réseau d'accueil et l'adresse principale du mobile.

10.8.3 L'adressage dans IPv6

Généralités

Dans un système de réseaux interconnectés, seul un adressage hiérarchique permet l'allégement des tables de routage, chaque routeur ne traitant que la partie de l'adresse correspondant à son domaine. Cependant, dans une communauté aussi vaste que celle d'Internet, l'adressage hiérarchique devient vite sans signification, aussi entre l'adressage à plat non-significatif d'IPv4 et l'adressage hiérarchique, tel que X.121, un compromis a été réalisé. L'adressage IPv6 comporte trois ensembles d'information. Le premier, sur 48 bits, est une agrégation hiérarchique de préfixes décrivant la connectivité du site, ce champ est désigné sous le terme topologie publique (identifiant des prestataires). Le second, sur 16 bits, décrit la topologie locale du site enfin le dernier, sur 64 bits, identifie de manière unique au monde une interface. Cet adressage est dénommé adressage agrégé ou *Aggregatable Global Unicast Address Format*.

Notation et type d'adresse

Une notation hexadécimale, sur 16 bits séparés par 2 points « : », remplace la notation décimale pointée d'IPv4. L'adresse passe de 32 à 128 bits, 8 mots de 16 bits. Ainsi, une adresse IPv6 est

18. C'est le cas notamment de NFS (*Network System File*) qui est un véritable système de gestion de fichier à travers un réseau IP.

© Dunod – La photocopie non autorisée est un délit

de la forme :

FE0C:DA98:0:0:0:0:5645:376E

L'écriture peut être simplifiée en remplaçant une succession de 0 par « :: », l'abréviation « :: » ne pouvant être utilisée qu'une seule fois. Ainsi, l'adresse précédente devient :

FE0C:DA98::5645:376E

IPv6 adopte une notation similaire à celle du CIDR, le champ préfixe étant désigné par un nombre représentant la longueur en bits du préfixe, l'écriture est donc de la forme : @IPv6/ longueur du préfixe en bits, soit par exemple

FE0C:DA98/32

FE0C:DA98:0:0/64

FE0C:DA98::/64

Très pénalisant en terme de performance réseau, la notion de broadcast disparaît. Elle est remplacée par une généralisation des adresses multicast. IPv6 distingue trois types d'adresse :

– les adresses *unicast* : une adresse unicast désigne une interface, elle peut être utilisée pour identifier un groupe d'interfaces lorsque ces interfaces constituent une agrégation de liens et doivent être vues comme une seule interface ;
– les adresses *multicast* (FF00::/8) : ces adresses désignent un ensemble d'interfaces dont la localisation n'est pas nécessairement sur le même réseau physique. Un datagramme adressé à une adresse multicast est acheminé à toutes les interfaces du groupe ;
– les adresses *anycast* : ces adresses introduites par IPv6 correspondent à une restriction des adresses de multicast. Elles désignent un ensemble d'interfaces partageant un même préfixe réseau. Cependant, lorsqu'un datagramme est adressé à une adresse anycast, il n'est délivré qu'à une seule interface du groupe, celle dont la métrique, au sens routage du terme, est la plus proche du nœud source.

Le plan d'adressage

➤ L'identifiant d'interface

L'indentifiant d'interface dans IPv6 correspond à la notion d'Host_ID d'IPv4. Afin de faciliter les opérations d'autoconfiguration et de disposer d'un identifiant unique au niveau mondial, l'identifiant correspond à une nouvelle proposition d'extension de l'adressage IEEE sur 64 bits. Ce nouvel identifiant d'interface sur 64 bits (*EUI-64, End-User Interface*) garantit l'unicité d'adresse. Pour les interfaces non dotées de cet identifiant, celui-ci peut être déduit de l'adresse MAC IEEE de 48 bits (figure 10.76).

Lorsqu'une interface n'est dotée d'aucun identifiant, l'administrateur local peut lui attribuer un identifiant, le bit U[19] est alors positionné à 0.

19. La signification du bit U est inversée par rapport à celle du bit U/L utilisée dans l'adressage MAC-48.

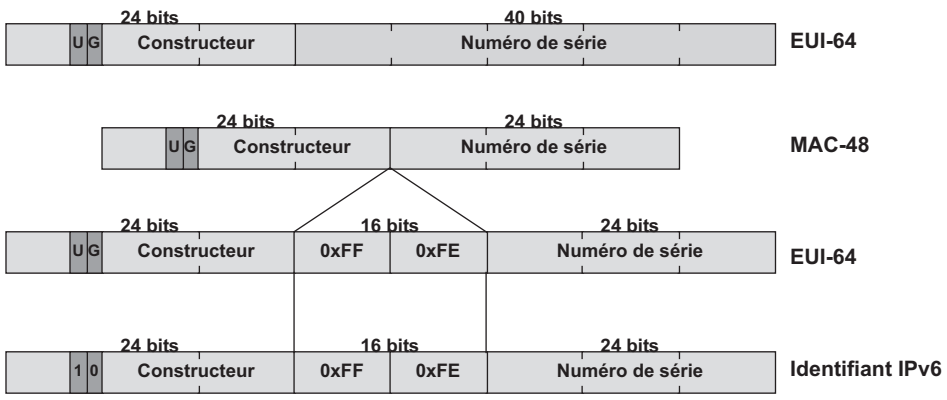


Figure 10.76 Construction de l'identifiant IPv6 à partir de l'adresse MAC.

➤ Les adresses spécifiques

Comme dans IPv4 certaines adresses ont une signification particulière, ce sont :

– L'adresse dite indéterminée (*unspeccified address*), cette adresse correspond à l'adresse 0.0.0.0 d'IPv4, elle désigne une interface en cours d'initialisation. Cette adresse 0:0:0:0:0:0:0:0 ou :: ne doit jamais être attribuée à une interface.

– L'adresse de bouclage (*loopback address*) correspond à l'adresse 127.0.0.1 d'IPv4, elle vaut 0:0:0:0:0:0:0:1 ou encore ::1.

➤ Les adresses dites de site local

Les adresses de site local (FEC0 ::/10) correspondent aux adresses privées d'IPv4 (RFC 1918, adresses de type 10.0.0.0). À l'instar d'IPv4, ces adresses ont une portée limitée au réseau privé, elles ne peuvent être utilisées pour se connecter à Internet (figure 10.77). Le champ Subnet_ID[20] permet à l'administrateur local de hiérarchiser son réseau.

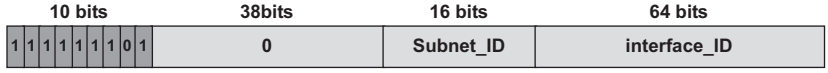


Figure 10.77 L'adressage de site local (adressage privé).

➤ Le plan d'adressage agrégé

L'adressage agrégé se présente comme étant un compromis entre un adressage hiérarchique strict et un adressage à plat. Il instaure une hiérarchie vis-à-vis des fournisseurs d'accès. Le premier niveau de hiérarchisation (**TLA**_id, *Top Level Aggregator*) sur 13 bits correspond à l'identification du fournisseur d'accès de transit à Internet. Le champ suivant sur 24 bits (**NLA**_id, *Next Level Aggregator*) est un champ d'agrégation dont le découpage est défini par l'autorité désignée dans le champ précédent. La dernière partie champ du NLA désigne le site local connecté au fournisseur d'accès. Le dernier champ d'agrégation (**SLA**_id, *Site Level*

20. Le terme Net_ID a été repris ici pour des raisons de compréhension. L'appellation officielle de champ en IPv6 est SLA (*Site Level Aggregator*).

© Dunod – La photocopie non autorisée est un délit

Aggregator) sur 16 bits permet au gestionnaire du site de hiérarchiser son plan d'adressage. Devant la difficulté de dimensionner les champs TLA et NLA, un champ de 8 bits a été prévu pour permettre le débordement à droite (TLA) ou à gauche (NLA) des champs TLA et NLA. La figure 10.78 représente ce type d'adresse.

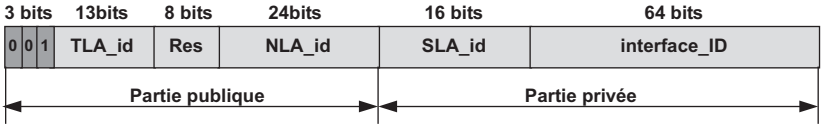


Figure 10.78 L'Adressage agrégé.

➤ L'adressage multicast

Afin d'éviter l'usage intempestif de broadcast qui pénalise les performances, IPV6 a généralisé la notion de multicast en définissant différents niveaux de diffusion. Une adresse multicast désigne un ensemble de nœuds, elles sont dites aussi adresses sur abonnement. L'adresse multicast comporte 4 champs (figure 10.79), le premier identifie une adresse de multicast (préfixe FF00::/8). Le second, le champ flags, est un champ de bits (4 bits) dont seul de dernier est défini, il s'agit du bit T. Ce bit à « 0 » indique que l'adresse est permanente. Le champ suivant indique le niveau de diffusion (*scope*). Les différentes valeurs de ce champ sont :

– 0, réservé ;
– 1, nœud local ;
– 2, lien local ;
– 5, site local ;
– 8, l'organisation locale ;
– E, global.

Figure 10.79 L'adressage multicast

Certaines adresses multicast ont été prédéfinies, ce sont notamment les adresses de diffusion des protocoles de routage. Chaque protocole de routage possède sa propre adresse.

➤ L'adressage d'anycast

Concrètement, une adresse anycast résulte de la concaténation d'un préfixe désignant le sous-réseau adressé et d'un suffixe nul (figure 10.80). En principe, actuellement une adresse anycast ne peut être attribuée qu'à une passerelle.

Figure 10.80 L'adressage d'anycast.

➤ L'adressage de transition d'IPv4 vers IPv6

La migration d'IPv4 vers IPv6 ne peut être réalisée que progressivement. Durant un temps assez important les deux versions de protocoles devront cohabiter. Aussi, deux solutions ont été envisagées pour permettre d'utiliser les adresses IPv4 dans le domaine IPv6. La première (figure 10.81) dite IPv4 mappée est une représentation interne des adresses afin de permettre à des programmes IPv6 de fonctionner sur un réseau IPv4. La communication se faisant d'une machine IPv4 à IPv4.

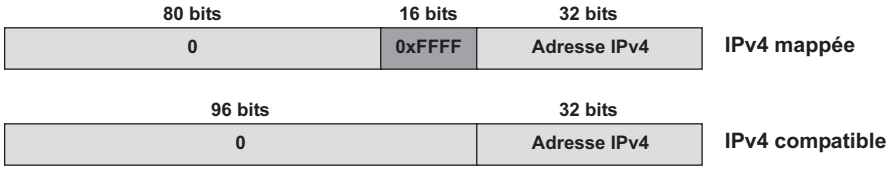


Figure 10.81 L'adressage IPv4/IPv6.

La seconde dite IPv4 compatible, permet à deux machines IPv6 de communiquer à travers un réseau IPv4 (tunnel IPv4). Le datagramme IPv6 d'adresse « : :a.b.c.d » est encapsulé dans un datagramme IPv4 d'adresse « a.b.c.d » (figure 10.81).

10.9 CONCLUSION

Le protocole TCP/IP est en principe un protocole d'extrémité. Les réseaux de transport (WAN), pour des raisons historiques et de performance, utilisent d'autres protocoles. TCP/IP est alors transporté en mode tunnel dans ces protocoles. L'étude de ces réseaux fait l'objet du chapitre suivant.

© Dunod – La photocopie non autorisée est un délit

EXERCICES

Exercice 10.1 Masque de sous-réseau

Une entreprise à succursales multiples utilise l'adresse IP 196.179.110.0. Pour une gestion plus fine de ses sous-réseaux, le responsable informatique désire pouvoir affecter une adresse IP propre à chaque sous-réseau des 10 succursales.

a) De quelle classe d'adressage s'agit-il ?

b) Donner et expliquez la valeur du masque de sous-réseau correspondant à ce besoin.

c) Combien de machines chaque sous-réseau pourra-t-il comporter et pourquoi ?

d) Définissez l'adresse de broadcast du sous-réseau 3 (expliquez) ?

Exercice 10.2 Masque de sous-réseau et dysfonctionnement

Certains utilisateurs du réseau local d'une entreprise, utilisant une application au-dessus de UDP, se plaignent de ne pas pouvoir communiquer avec tous les autres utilisateurs alors que ceux-ci le peuvent avec eux. Le responsable bureautique local vous demande d'expertiser son réseau. Pour lui le fait qu'une station puisse émettre des messages vers une autre et que cette dernière ne puisse répondre le laisse perplexe. Votre rapport d'expertise, à compléter, comporte les éléments suivants :

– vous constatez que toutes les stations sont sur le même segment Ethernet et que celui-ci ne comporte aucun routeur et qu'aucune station n'est configurée pour remplir ce rôle ;

– vous relevez les configurations suivantes :

Station A	@ 150.150.1.28	masque 255.255.255.0
Station B	@ 150.150.1.57	masque 255.255.0.0
Station C	@ 150.150.2.28	masque 255.255.255.0
Station D	@ 150.150.2.57	masque 255.255.0.0

– vous établissez la matrice de communication (complétez par oui, dans le tableau de la figure 10.82 lorsque la communication est possible et par non dans le cas contraire)

Source / Destination	150.150.1.28 (255.255.255.0)	150.150.1.57 (255.255.0.0)	150.150.2.28 (255.255.255.0)	150.150.2.57 (255.255.0.0)
150.150.1.28				
150.150.1.57				
150.150.2.28				
150.150.2.57				

Figure 10.82 Matrice de communication.

Exercice 10.3 (Table ARP)

L'un des établissements d'une entreprise utilise la plage d'adresse 10.0.0.0 de la classe A (RFC 1918). Si on considère 4 machines de cet établissement dont les noms et adresses sont donnés ci-dessous (figure 10.83) :

Nom	@IP	@MAC
Pierre.Entreprise.com	10.99.43.27	MAC_1
Jacques.Entreprise.com	10.163.12.254	MAC_2
Alfred.Entreprise.com	10.189.12.27	MAC_3
Martine.Entreprise.com	10.126.43.254	MAC_4

Figure 10.83 Plan d'adressage.

On vous demande :

a) Quel est le NET_ID de ce plan d'adressage ?

b) Quel est le nombre de bits nécessaires pour réaliser deux sous-réseaux (SubNet_ID) tels que Pierre et Martine appartiennent au même sous-réseau et que Jacques et Alfred appartiennent à un autre sous-réseau ? On rappelle que les bits du Net_ID et du SubNet_ID doivent être contigus. Donnez le masque correspondant.

c) Quel est le nombre de bits minimum et nécessaire pour qu'aucune des machines n'appartienne au même sous-réseau ? Donnez le masque correspondant.

d) Pour permettre la communication entre les deux sous-réseaux de la question b, on relie les brins Ethernet de ces deux sous-réseaux par un routeur configuré en proxy ARP (c'est lui qui répond en lieu et place des stations connectées sur ses autres liens). Si on affecte à chaque interface LAN de ce routeur la première adresse disponible (Net_Host=1), quelles sont les adresses affectées ? Représentez l'ensemble par un schéma.

e) En admettant que toutes les stations aient communiqué entre elles et qu'aucune entrée n'ait été effacée quel est le contenu de la table ARP de la station de Pierre ? Pour cette question on affectera des adresses MAC fictives à chaque interface du routeur : MAC_R1 et MAC_R2.

f) L'établissement envisage de raccorder son réseau à Internet. Est-ce possible en l'état. Quelle est la difficulté et quelle solution proposeriez-vous ?

Exercice 10.4 Trace TCP/IP

La trace reproduite ci-dessous (figure 10.84) a été réalisée sur réseau de type Ethernet. On vous demande de l'analyser et de fournir toutes les informations relatives au protocole utilisé. Dans la deuxième trame proposée, ne commentez que les parties intéressantes vis-à-vis de ce qui a déjà été commenté dans la première trame.

© Dunod – La photocopie non autorisée est un délit

```
Captured at:  +00:03.934
Length: 114    Status: Ok
OFFST DATA                                                  ASCII
0000: 00 A0 24 BD 75 DB 08 00 02 05 2D FE 08 00 45 00  ..$.u.....-...E.
0010: 00 60 3C EF 00 00 1C 06 A4 FE 80 00 64 01 D0 80  .`<.........d...
0020: 08 29 00 17 04 2B 47 A8 BA 20 01 A3 96 14 50 18  .)...+G.. ....P.
0030: 20 00 72 D3 00 00 FF FB 01 FF FD 01 0D 0A 0D 0A   .r.............
0040: 55 4E 49 58 28 72 29 20 53 79 73 74 65 6D 20 56  UNIX(r) System V
0050: 20 52 65 6C 65 61 73 65 20 34 2E 30 20 28 63 65   Release 4.0 (ce
0060: 76 73 61 30 30 29 0D 0A 0D 00 0D 0A 0D 00 9F 59  vsa00).........Y
0070: 6E FC                                             n.

Captured at:  +00:04.771
Length: 64    Status: Ok
OFFST DATA                                                  ASCII
0000: 00 A0 24 BD 75 DB 08 00 02 05 2D FE 08 00 45 00  ..$.u.....-...E.
0010: 00 29 3C F2 00 00 1C 06 A5 32 80 00 64 01 D0 80  .)<......3..d...
0020: 08 29 00 17 04 2B 47 A8 BA 62 01 A3 96 1B 50 18  .)...+G..b....P.
0030: 20 00 D2 14 00 00 63 00 00 08 00 00 69 55 A1 FF   .....c.....iU..
```

Figure 10.84 Trace TCP/IP.

La structure générale de l'encapsulation du datagramme IP dans une trame Ethernet est donnée figure 10.85.

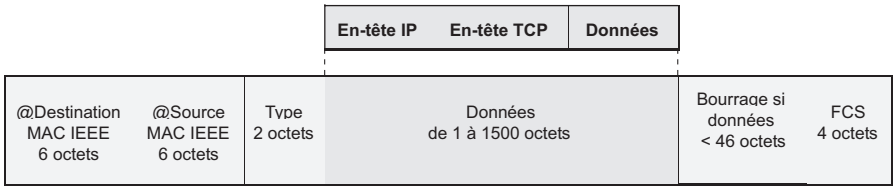


Figure 10.85 Encapsulation de TCP/IP dans une trame MAC Ethernet V2.

Chapitre **11**

Les réseaux de transport X.25, Frame Relay, ATM et boucle locale

Un réseau peut être vu comme étant la superposition de trois plans (figure 11.1) :

– Le **plan usager** qui correspond à l'installation privée de l'usager final.

– Le **plan service** qui correspond au point où le service requis par l'usager, service données ou voix, est mis à sa disposition. Ces réseaux peuvent être privés ou publics. L'usager est relié au plan service par une liaison d'abonné appelée aussi **boucle locale**. Les éléments actifs de ces réseaux (commutateurs, routeur...) ne sont pas reliés directement entre eux.

– Enfin, le **plan transmission** qui correspond au réseau réel de transport des données et de la voix. Ce sont les techniques de numérisation qui ont permis le transport de manière banalisée de tout type de flux. C'est à ce réseau que sont reliés les éléments actifs du réseau de transport.

Ce chapitre concerne l'étude des plans de transmission, de service et des modes d'accès à ce dernier. Les composantes du plan usager, réseaux locaux et téléphoniques, sont étudiées respectivement dans les chapitres 12 (*Réseaux locaux*), 15 et 16 (*Téléphonie*).

11.1 LE PLAN DE TRANSMISSION

11.1.1 Généralités

Jusqu'aux années 60, les réseaux étaient fondamentalement distincts, il était même interdit d'effectuer des transferts de données sur le réseau téléphonique. Avec la numérisation de la voix, les infrastructures se sont banalisées. La notion de réseaux de transmission de données indépendants du type de ces données était née (figure 11.2). Pour optimiser l'utilisation

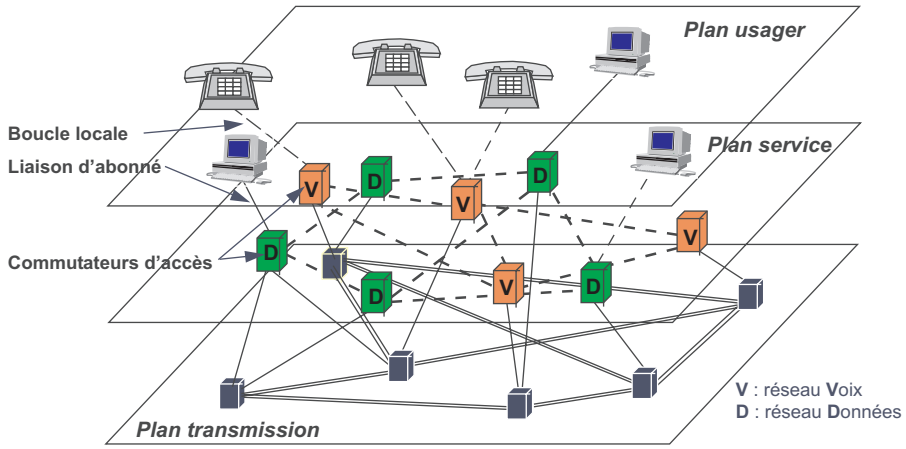


Figure 11.1 Les trois plans d'un réseau de transmission.

des supports de transmission, le CCITT (UIT-T) a normalisé, à partir des liaisons MIC[1], des niveaux de multiplexage. Cette hiérarchie appelée **PDH** (*Plesiochronous Digital Hierarchy*), différente aux États-Unis, a constitué la base de tous les réseaux de transmission jusqu'aux années 90.

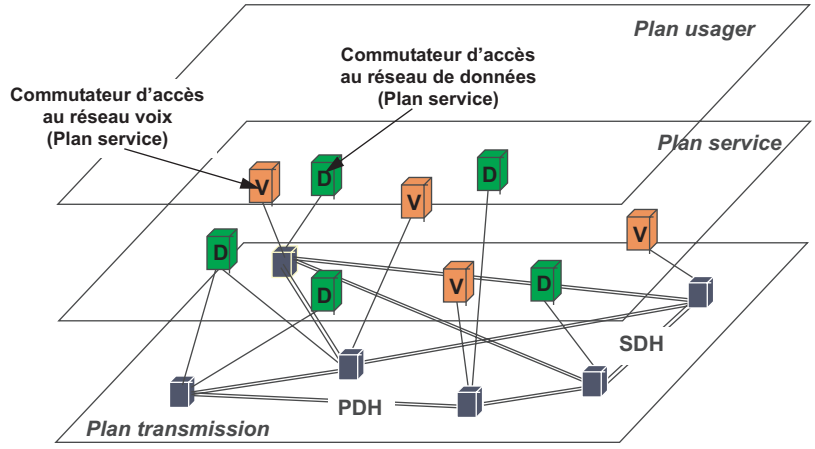


Figure 11.2 Le plan de transmission.

Outre la rationalisation de l'utilisation des supports, la hiérarchie PDH a eu le mérite de résoudre les difficultés de synchronisation des flux provenant de sources différentes aux horloges proches (plésio) mais non identiques. Fondée sur un réseau de distribution d'horloge, la hiérarchie synchrone (**SDH**, *Synchronous Digital Hierarchy*) garantit la délivrance de bits en synchronisme d'une horloge de référence. Elle autorise des débits plus élevés et répond à un besoin de normalisation des interfaces optiques.

1. Voir section 7.3.3, *Exemple d'application : la trame MIC*.

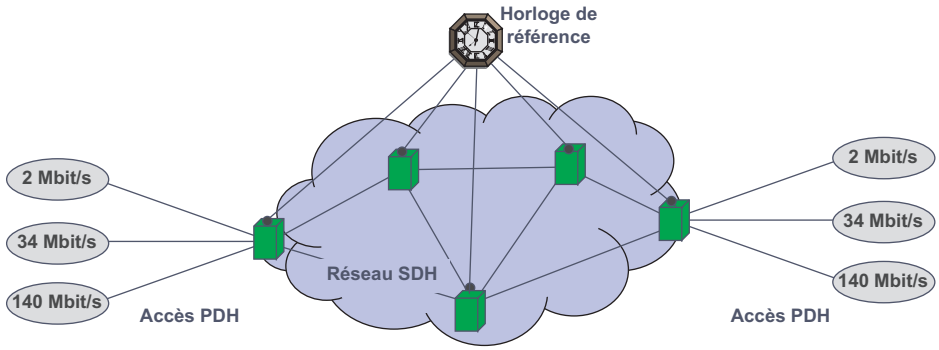


Figure 11.3 Cohabitation des techniques PDH et SDH.

Si les cœurs de réseaux sont aujourd'hui **SDH**, pour des raisons historiques, la distribution des débits chez l'utilisateur repose sur la hiérarchie plésiochrone. L'adage qu'une technologie ne supplante jamais une autre mais vient la compléter prend ici toute sa valeur (figure 11.3).

11.1.2 La synchronisation des réseaux

Horloges et mécanismes associés

➤ Les différences d'horloges et leurs conséquences

Les références temporelles dans un réseau sont fournies à partir d'oscillateurs. Indépendamment du fait qu'il n'est pas possible de réaliser des oscillateurs de fréquences strictement identiques, les signaux d'horloge déduits du signal binaire subit les mêmes altérations que ce dernier. Même, lorsque les différentes horloges du réseau sont asservies par une horloge de référence unique, des écarts d'horloge subsistent. Les différences d'horloge provoquent des différences de débits (figure 11.4) et sont, aujourd'hui, la principale source d'erreur dans les réseaux (**saut de bits**).

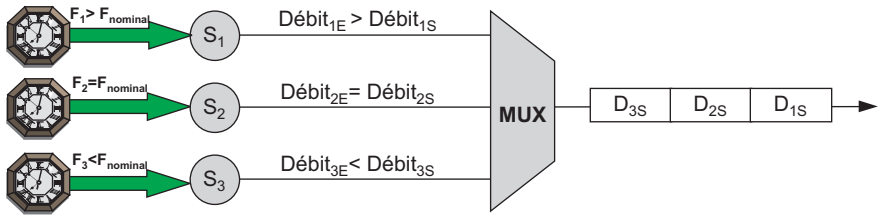


Figure 11.4 Écarts d'horloge et de débit.

➤ Les mécanismes de correction d'horloge

Les signaux d'horloge subissent deux types d'altération, l'une et l'autre correspondent à des variations de la fréquence d'horloge autour d'une valeur moyenne.

La première est une variation rapide autour de la fréquence nominale, le cycle est répétitif plusieurs fois par seconde, il s'agit du phénomène connu sous le nom de **gigue**[2] ou *jitter* . La

2. La gigue, dans les réseaux, a deux origines. Celle évoquée ici correspond aux fluctuations d'horloge, elle est quan-

© Dunod – La photocopie non autorisée est un délit

gigue s'exprime en amplitude (variation autour de la fréquence moyenne), de l'ordre de 10^{-5} à 10^{-6}, et en fréquence.

La seconde, beaucoup plus lente, s'appelle dérapage ou glissement, son cycle peut être très grand, c'est par exemple la variation de fréquence due aux variations de température durant la journée.

Pour remédier à ces écarts d'horloge et donc de débit, plusieurs solutions sont envisageables. La plus simple consiste à régénérer périodiquement le signal, les **répéteurs** ou **régénérateurs**, non seulement restaurent le signal (forme et amplitude) mais peuvent aussi recalibrer le signal autour d'une fréquence moyenne (figure 11.5).

Figure 11.5 Régénération du signal par un répéteur.

Cependant, les bits sont reçus par les éléments actifs au rythme de l'horloge source. Si celle-ci est supérieure à celle de l'horloge émission, il est nécessaire de mémoriser les bits excédentaires en attente d'une dérive inverse de l'horloge source. En moyenne, les bits reçus ne peuvent excéder les bits émis. Pour limiter la taille des mémoires tampons, l'UIT-T a fixé des limites aux dérives d'horloge, la stabilité des horloges devant être d'autant plus grande que les débits sont importants.

La figure 11.6 représente un système de correction de gigue. La mémoire tampon (*buffer*) de réception est constituée par un registre à décalage « élastique ». Le *buffer* est plus ou moins rempli selon les écarts de rythme entre l'horloge de réception (Hr) et l'horloge d'émission (He). Ce dispositif est efficace mais introduit un retard (temps de rétention des bits).

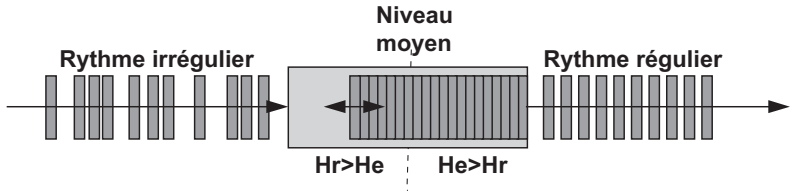


Figure 11.6 Principe de la correction de gigue d'horloge.

Lors des opérations de multiplexage, les différentes voies incidentes peuvent avoir des rythmes d'horloge différents. Les dispositifs précédents ne suffisent plus. La seule solution envisageable est alors de prévoir dans le train d'émission un cadrage variable des débits affluents. Ce principe, illustré par la figure 11.7, est utilisé aussi bien dans la hiérarchie plésiochrone (justification au niveau bit) que dans la hiérarchie synchrone (justification au niveau octet). Un pointeur permet de déterminer où débutent les données.

tifiable et engendre des décalages temporels entre les bits provoquant éventuellement des erreurs (saut de bits). L'autre, dépend essentiellement de la charge du réseau et de ses variations, elle n'engendre pas d'erreur binaire mais peut rompre, éventuellement, l'isochronie des paquets de données.

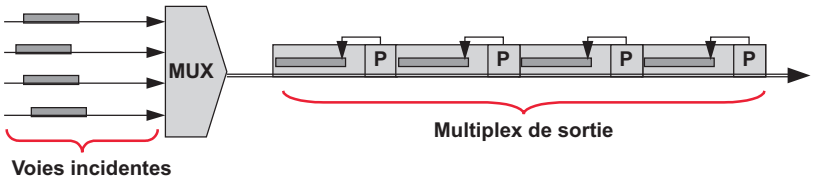


Figure 11.7 Principe de la justification.

Afin de permettre le cadrage des données, le débit du multiplex de sortie est nécessairement plus élevé que la somme des débits des voies incidentes, ce surdébit est dit surdébit de justification. Notons que seule l'utilisation d'un pointeur et donc du surdébit est capable de compenser les écarts de phase introduits par les différences de trajet (temps de propagation) des différents affluents.

La distribution d'horloge dans un réseau SDH

Il existe deux modes de synchronisation des réseaux. Le mode synchronisation mutuelle et le mode maître-esclave ou hiérarchique. Dans le mode synchronisation mutuelle, tous les nœuds du réseau sont considérés au même niveau. Chaque nœud détermine, à partir des signaux incidents, une horloge moyenne et y aligne la sienne. Cette méthode est peu utilisée, on lui préfère une synchronisation de type hiérarchique. Le réseau de distribution d'horloge[3] est organisé sur trois niveaux (figure 11.8). Le rythme de référence primaire (**PRC**, *Primary Reference Clock*, horloge primaire de référence) est fourni par une horloge au césium de grande stabilité (10^{-11}). À des fins de sécurité, cette horloge est doublée. Certains opérateurs utilisent des récepteurs **GPS** (*Global Positionning System*). Cette dernière approche, bien qu'elle soit sous le contrôle du ministère de la défense américain (DoD), tend à se répandre. Le GPS peut être utilisé comme horloge principale mais, le plus souvent, il est employé comme horloge de secours.

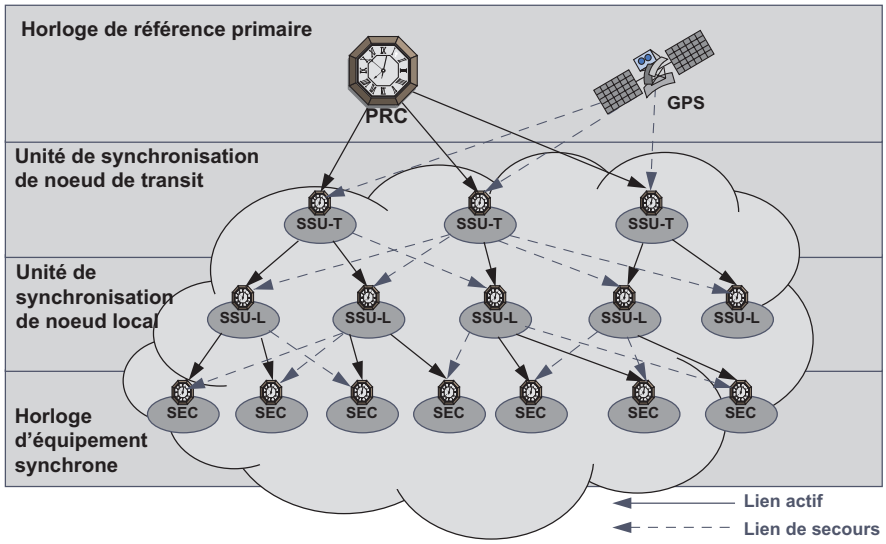


Figure 11.8 Synchronisation maître-esclave dans un réseau SDH.

3. La distribution d'horloge n'est pas réservée aux réseaux SDH, elle peut l'être aussi dans les réseaux PDH.

© Dunod – La photocopie non autorisée est un délit

La configuration du réseau de distribution d'horloge doit assurer une redondance des liens afin de rétablir un lien de synchronisation en cas de défaillance d'un nœud de niveau supérieur. Le tableau de la figure 11.9 détaille les différents niveaux de distribution d'horloge, il indique les normes de référence et la stabilité des horloges de chaque niveau.

Abréviation	Appellation	Avis UIT-T	Stabilité
PRC	*Primary Reference Clock* Horloge primaire de référence	G.811	10^{-11} sur le long terme
SSU-T	*Synchronisation Supply Unit Transit* Unité de synchronisation de nœud de transit	G.812T	50.10^{-10} Dérive maxi. sur 24 H. 10^{-9}
SSU-L	*Synchronisation Supply Unit Local* Unité de synchronisation de nœud de transit	G.812L	10^{-8} Dérive maxi.sur 24 H. 2.10^{-8}
SEC	*Synchronous Equipement Clock* Horloge d'équipement synchrone	G.813	5.10^{-8} Dérive sur 24 H. 2.10^{-7}

Figure 11.9 Références normatives.

Dans les réseaux SDH, l'octet **SSM** (*StatuS Message Byte*, message d'état de la synchronisation) permet à chaque instant d'être informé de l'état de la source de synchronisation. Enfin, remarquons que pour garantir leur indépendance chaque opérateur dispose de sa propre horloge de référence. Par conséquent, si les réseaux d'opérateur sont des réseaux synchrones (SDH), le réseau qui résulte de leur interconnexion est un réseau du type plésiochrone.

11.1.3 La hiérarchie plésiochrone (PDH)

Généralités

La hiérarchie PDH est apparue avec la numérisation de la voix et la nécessité de transporter simultanément plusieurs canaux téléphoniques sur un même support (multiplexage temporel). Le multiplex de base est constitué du regroupement de plusieurs canaux téléphoniques de 64 kbit/s. Les regroupements sont différents en Europe, au Japon et aux États-Unis, ce qui a conduit à la définition de différentes hiérarchies plésiochrones illustrées par la figure 11.10.

Chaque intervalle de temps ou IT peut transporter un échantillon de voix ou toute autre information numérique. La concaténation de plusieurs voies permet une granularité des débits modulo 64 kbit/s. Les surdébits entre les différents niveaux de regroupement sont dus aux signaux d'alignement, de supervision et de justification binaire. Les niveaux 5 ne sont pas normalisés par l'UIT-T.

La trame de base du système européen

La trame de base regroupe 30 voies de communication (Intervalles de Temps, IT ou *slot time*) et 2 voies de service de 8 bits. La position de chaque voie est déterminée en comptant un certain nombre de temps d'horloge à partir d'une combinaison particulière de bits appelée **mot de verrouillage de trame** (**MVT**) qui balise le début de la trame de 32 voies (IT). L'organisation de base de la trame (G.704) est illustrée par la figure 11.11.

Les trames sont regroupées selon une structure dite de **multitrame**, cette structure regroupe deux sous-groupes de 16 trames numérotées globalement de 0 à 31. Ce regroupement permet le transport d'informations spécifiques notamment un contrôle d'erreur sur 4 bits émis bit par bit

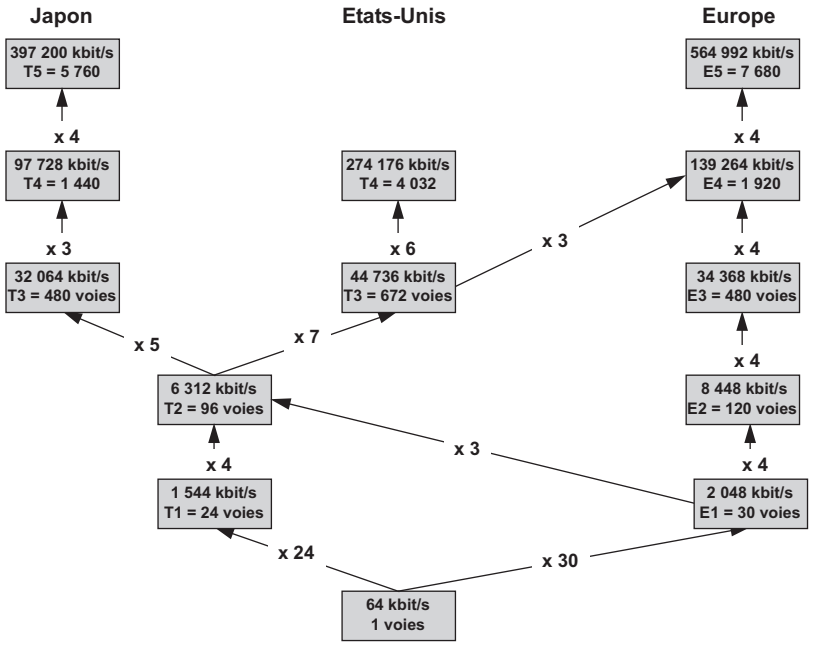


Figure 11.10 Les différents regroupements en hiérarchie PDH.

dans le premier bit de chaque IT0 (bit X de la figure 11.11). L'IT0 des trames paires transporte une information de synchronisation dite mot de verrouillage de trame ou MVT (0011011). Les bits P et D des trames impaires transportent une information d'alarme (P, alarme urgente ; D, alarme non urgente). Enfin, les bits YYYY sont laissés à disposition pour un usage national. L'IT16 de la trame 0 sert de fanion pour indiquer le début d'une séquence de 16 trames (**mot de verrouillage multitrame**). Le bit A est utilisé pour signaler une perte d'alignement de la multitrame.

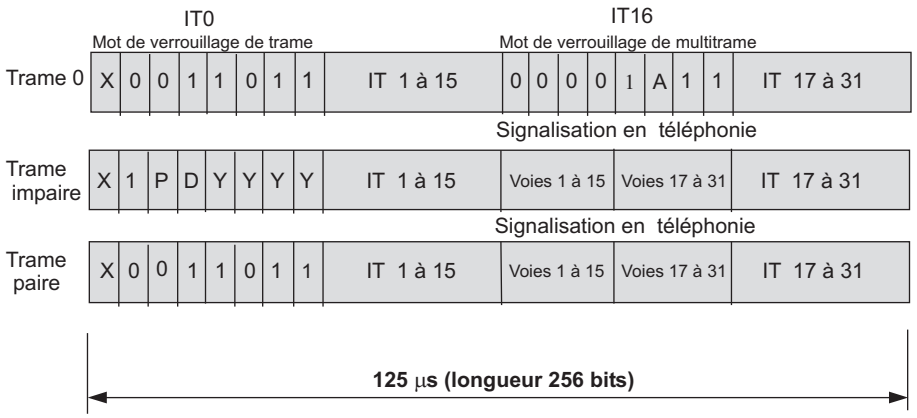

IT0
Mot de verrouillage de trame
IT16
Mot de verrouillage de multitrame
Trame 0
X 0 0 1 1 0 1 1
IT 1 à 15
0 0 0 0 1 A 1 1
IT 17 à 31
Signalisation en téléphonie
Trame impaire
X 1 P D Y Y Y Y
IT 1 à 15
Voies 1 à 15
Voies 17 à 31
IT 17 à 31
Signalisation en téléphonie
Trame paire
X 0 0 1 1 0 1 1
IT 1 à 15
Voies 1 à 15
Voies 17 à 31
IT 17 à 31
125 µs (longueur 256 bits)

Figure 11.11 Organisation de la trame G.704 ou G.732 (téléphonie).

© Dunod – La photocopie non autorisée est un délit

La trame de base du système américain

La trame nord-américaine (utilisée aussi au Japon) ou T1 comporte 24 IT de 64 kbit/s donnant un débit total de 1 544 kbit/s et un débit utile de 1 536 kbit/s.

À l'instar de la trame G.704, la signalisation comporte deux types d'informations, celles relatives à la structure de la trame (ou **signalisation de supervision**) et celles en rapport avec l'état de chaque canal téléphonique (**signalisation voie par voie** ou CAS).

La trame de base T1[4] (trame G.733, aussi notée DS1 à DS12), représentée figure 11.12, comprend 24 IT (DS0) de 8 bits (192 bits). La multitrame de premier niveau regroupe 12 trames de base. Chaque trame de base est précédée d'un bit (bit de tramage constituant la signalisation de supervision). Ces 12 bits forment un mot (mot **SF**, *SuperFrame*) représentant la séquence binaire 100011001100 et identifiant la trame.

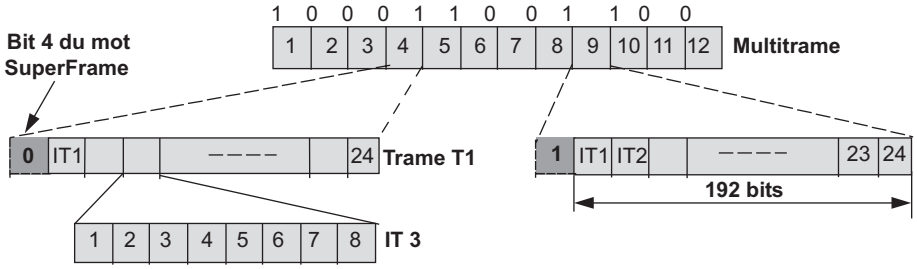


Figure 11.12 Organisation de la multitrame T1.

La signalisation téléphonique de chacune des voies est réalisée par vol, toutes les 6 trames, du bit de poids faible dans l'IT (un bit de signalisation est substitué au bit d'information, c'est une signalisation dans la bande). Remarquons que, si en téléphonie ce mode de signalisation est efficace puisqu'il économise un IT, en transmission de données, il pénalise fortement le système, la bande utile n'étant que de 56 kbit/s par IT (7 bits, toutes les 125 μs).

11.1.4 La hiérarchie synchrone (SDH)

Généralités

Outre l'utilisation d'un surdébit (justification et bourrage) qui consomme inutilement de la bande passante, l'inconvénient majeur de la hiérarchie PDH réside dans l'obligation de démultiplexer complètement le train à haut débit pour reconstituer un lien à 2 Mbit/s. La figure 11.13 illustre l'extraction d'un conduit à 2 Mbit/s d'un lien à 140 Mbit/s.

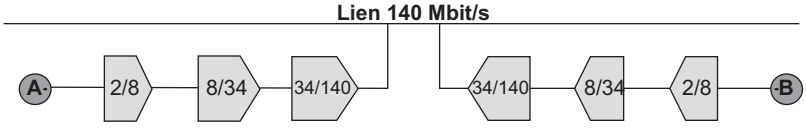


Figure 11.13 Constitution d'une liaison à 2 Mbit/s entre A et B en PDH.

4. T1 désigne le canal de transmission, DSx le format des données.

La hiérarchie synchrone se distingue essentiellement de la hiérarchie plésiochrone par la distribution d'horloge à tous les niveaux du réseau réduisant les écarts d'horloge. Les signaux sont encapsulés dans un « *container* ». À chaque *container* est associé un surdébit destiné à l'exploitation de celui-ci. Le container et le surdébit constituent un container virtuel (**VC**, *Virtual Container*). Un pointeur (surdébit) pointe sur la charge utile de la trame. Lorsque l'horloge source n'est pas en phase avec l'horloge locale, la valeur du pointeur est incrémentée ou décrémentée. L'utilisation de ces pointeurs permet d'insérer ou d'extraire un train numérique de différents débits sans être contraint de reconstituer toute la hiérarchie de multiplexeurs (figure 11.14). Ce dernier point constitue l'un des principaux avantages de la hiérarchie SDH par rapport à la hiérarchie PDH.

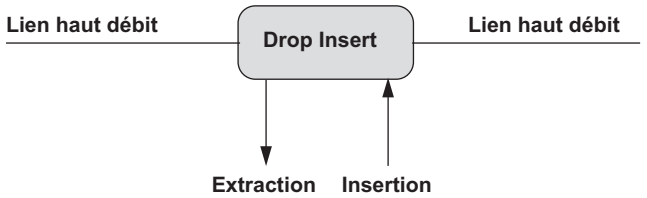


Figure 11.14 Insertion et extraction d'un niveau inférieur.

On distingue deux types de hiérarchie synchrone : la hiérarchie SDH en Europe et la hiérarchie **SONET**[5] (*Synchronous Optical NETwork*) aux États-Unis. Pour garantir la connectivité des différentes hiérarchies, des niveaux identiques ont été définis. Le premier niveau de la hiérarchie SONET : **STS-1** (*Synchronous Transport Signal - level 1*) ou **OC1** (*Optical Carrier-1*) est défini à 51,84 Mbit/s. La hiérarchie SDH fixe un premier niveau (ou trame de base) à 155,52 Mbit/s (**STM-1**, *Synchronous Transport Module - level 1*). Le tableau de la figure 11.15 donne la correspondance entre les deux hiérarchies.

SONET	SDH	Débit en Mbit/s	Accès ATM
OC1		51,84	
OC3	**STM-1**	**155,52**	Oui
OC9		466,56	
OC12	**STM-4**	**622,08**	Oui
OC18		933,12	
OC24		1 244,16	
OC36		1 866,24	
OC48	**STM-16**	**2 488,32**	Oui

Figure 11.15 Correspondance entre SONET et SDH.

La trame de base SDH (figure 11.16) comporte 2 430 octets émis avec une période de récurrence de 125 μs soit un débit de 155,20 Mbit/s. Elle est divisée en neuf éléments ou rangées de 270 octets, chaque élément est divisé en deux champs. Un champ de surdébit de 9 octets par rangée (**SOH**, *Section OverHead*) contient les informations de supervision, notamment les pointeurs. Les données sont déposées dans les champs utiles (261 octets) de chacune des rangées (**AU**, *Administrative Unit*). L'ensemble des données déposées forme un *container*.

5. C'est la hiérarchie SONET qui, issue des travaux de Bellcore en 1985 (*BELL COmmunication REsearch*), est à l'origine de la hiérarchie SDH.

© Dunod – La photocopie non autorisée est un délit

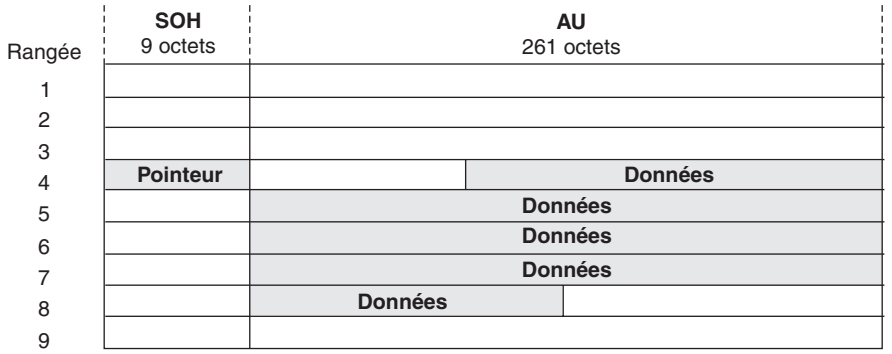


Figure 11.16 Structure simplifiée de la trame SDH.

Les équipements SDH

La hiérarchie synchrone met en œuvre trois types d'équipements (figure 11.17) :

– Les **multiplexeurs d'accès** permettent le multiplexage et le démultiplexage de plusieurs affluents plésiochrones et/ou synchrones.

– Les **multiplexeurs à insertion/extraction** (**ADM**, *Add Drop Mux*) assurent le transfert des données d'Est en Ouest (E ↔ W) tout en autorisant l'extraction et/ou l'insertion de sous-débit.

– Les **brasseurs numériques** (**DXC**, *Digital Cross Connect*) modifient l'affectation des flux d'information entre un affluent d'entrée et un affluent de sortie. Le croisement de flux est défini par l'opérateur, il est permanent.

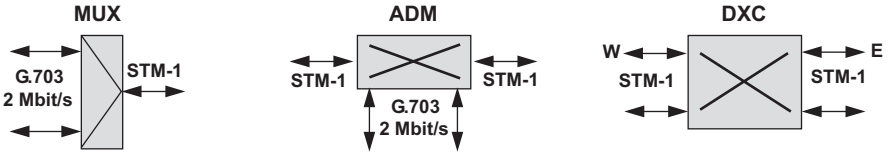


Figure 11.17 Les équipements SDH.

Le multiplexage des différents affluents d'ordre N vers un affluent d'ordre $N + 1$ est réalisé par entrelacement d'octets (figure 11.18).

L'entrelacement temporel d'octets permet d'une part, en répartissant les erreurs, d'en améliorer la détection et, d'autre part facilite l'extraction/insertion, il n'est pas nécessaire d'attendre la réception complète de l'affluent pour débuter son insertion/extraction dans le multiplex d'ordre supérieur/inférieur.

Topologie d'un réseau SDH

La technologie SDH peut être mise en œuvre sur toutes les formes de topologie : point à point, arborescente, bus, anneau et maillée. Généralement, les réseaux dorsaux utilisent une topologie maillée alors que les réseaux de desserte (métropolitain) sont constitués d'une hiérarchie d'anneaux (figure 11.19).

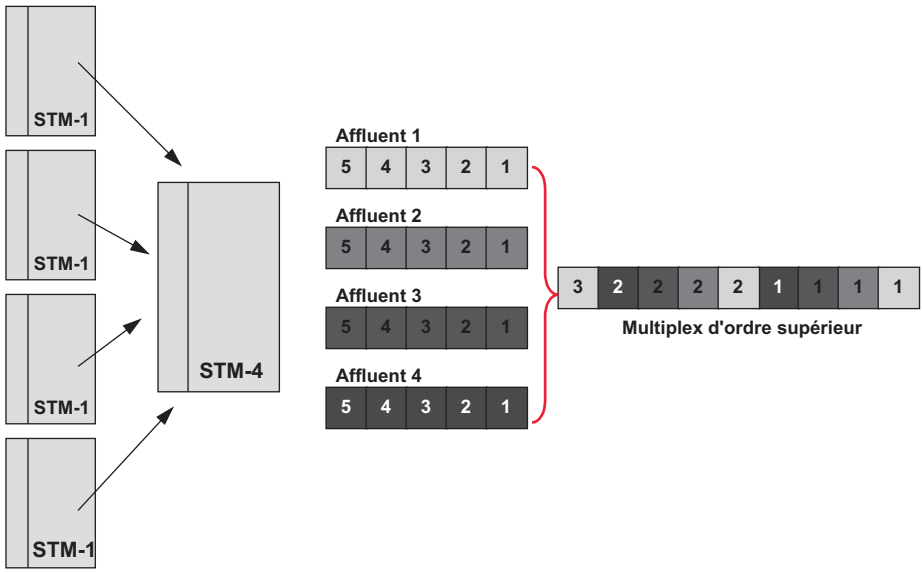


Figure 11.18 Principe du multiplexage d'octets.

Un autre avantage des infrastructures SDH concerne les mécanismes de sécurisation automatique qui permettent le rétablissement du trafic dans des délais d'environ 50 ms. Ce mécanisme, dit **d'autocicatrisation** (**APS**, *Automatic Protection Swiching*), est basé sur l'utilisation d'informations de supervision contenues directement dans l'en-tête SDH (surdébit de section, SOH).

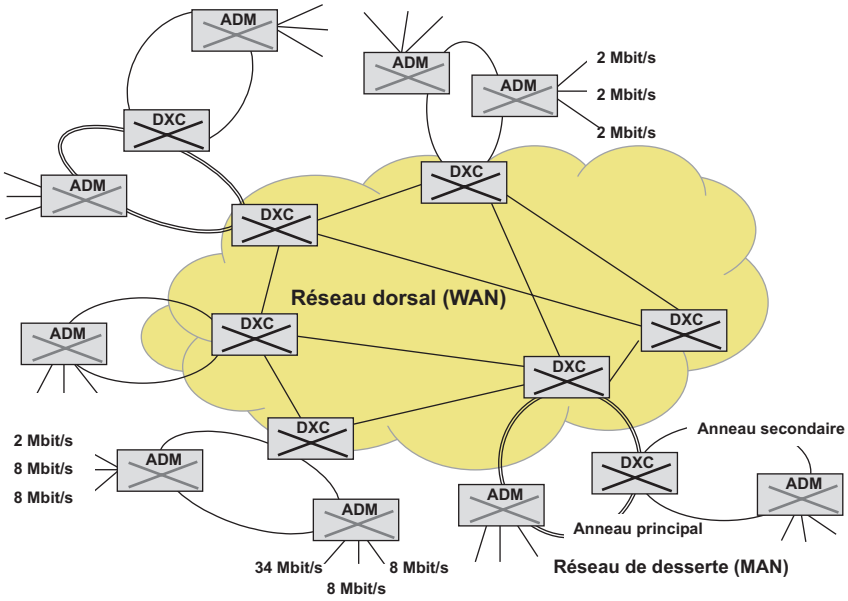


Figure 11.19 Principe d'un réseau SDH.

© Dunod – La photocopie non autorisée est un délit

La transmission optique

Si SDH se préoccupe de la structuration des données, la transmission physique est aujourd'hui optique. L'apparition des systèmes WDM/DWDM *(Wavelength Division Multiplexing, Dense WDM*) illustré figure 11.20 permet sur une seule fibre de disposer jusqu'à 128 canaux de communication. Les amplificateurs optiques dopés à l'erbium (EDFA, *Erbium Doped Fiber Amplifier*) compensent les pertes d'insertion dues aux opérations de multiplexage et de démultiplexage.

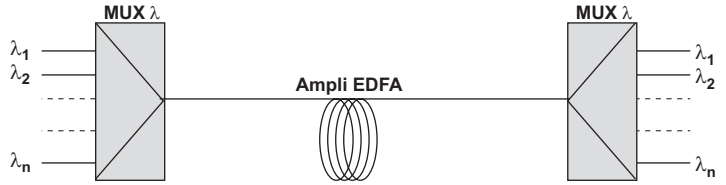


Figure 11.20 Principe d'une liaison DWDM.

11.2 LE PLAN DE SERVICE

11.2.1 Généralités

Le plan de service (figure 11.21) correspond au réseau de transport de données. L'interconnexion des installations locales de l'usager est réalisée par le plan service. La figure 11.22 représente le réseau de transport tel que le voit l'usager.

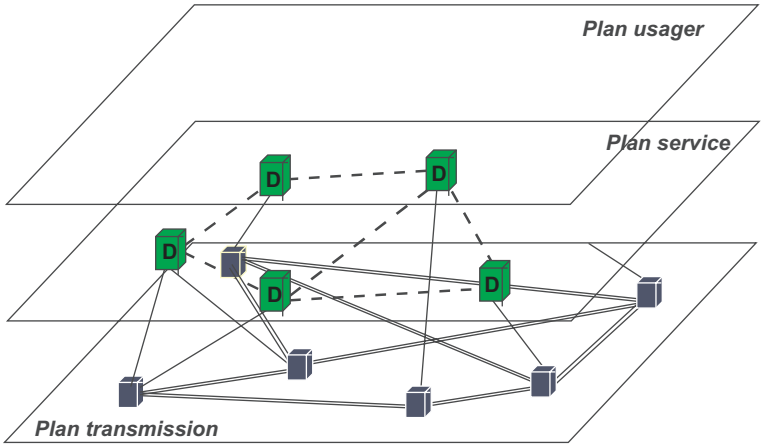


Figure 11.21 Le plan de service.

Au cours des années 70, la recherche de la performance a orienté les concepteurs de réseaux vers la réalisation de réseaux à commutation de paquets (*packet switching*) en mode orienté connexion (**CONS**, *Connection Oriented Network Service*) avec le protocole X.25. Défini au départ comme protocole d'accès, X.25 a très vite évolué vers un protocole de cœur de réseau. Le besoin croissant de bande passante a conduit les opérateurs à rechercher des protocoles internes plus efficaces. À cet effet, les protocoles internes ont d'abord évolué vers le relais de trame (**FR**, *Frame Relay*), puis vers **l'ATM** (*Asynchronous Transfer Mode*).

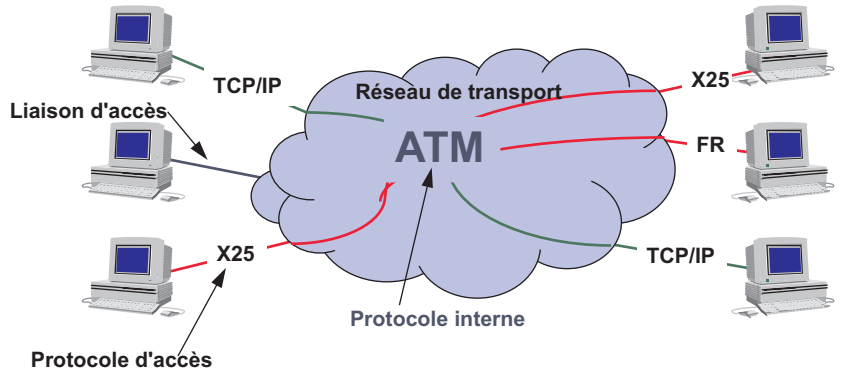


Figure 11.22 Protocoles d'accès et protocole interne.

Cependant, afin de garantir la pérennité des services et de faire bénéficier les usagers des progrès technologiques, les accès X.25 ont été maintenus et des accès FR et TCP/IP ont été offerts (figure 11.23). Deux modes d'accès aux réseaux publics sont définis :

– Les modes d'accès permanent (*On-line*), l'utilisateur est alors relié au réseau via une ligne dédiée (liaison spécialisée).

– Les modes d'accès temporaire (*Dial-up*), l'utilisateur accède alors au réseau via le réseau téléphonique (RTC ou RNIS).

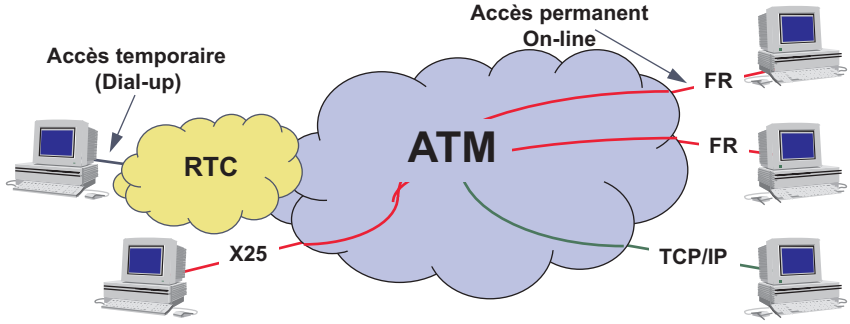


Figure 11.23 Les différents modes d'accès au réseau de transport.

11.2.2 Le protocole X.25 [6]

Généralités

Conçu par les PTT français et britanniques, TCTS (*Trans Canada Telephon System*) et Telnet (USA), le protocole X.25 a été le premier protocole utilisé dans les réseaux publics de données. C'est en décembre 1978 que Transpac (filiale de France Télécom) a ouvert le premier réseau mondial public de transmission en mode paquets X.25 (**PSPDN**, *Packet Switched Public Data*

6. Nous avons pris ici le parti de maintenir une étude détaillée de X.25. En effet, le protocole X.25 est l'archétype des protocoles réseau, il permet d'expliquer simplement tous les mécanismes. Protocole des années 80, X.25 reste et restera longtemps encore un protocole très utilisé. X.25 est aux protocoles de télécommunications ce que Cobol est aux langages de programmation.

© Dunod – La photocopie non autorisée est un délit

Network). L'avis **X.25** adopté en septembre 1976 par le CCITT (UIT-T) définit les protocoles d'accès au réseau, c'est-à-dire le protocole entre l'ETTD (DTE) et le réseau (ETCD ou DCE dans la norme X.25).

Le protocole X.25 couvre les trois premières couches du modèle OSI (figure 11.24) :

– La couche physique, niveau bit ou X.25-1 définit l'interface ETTD/ETCD. Elle est conforme à l'avis X.21 et X.21 bis de l'UIT-T.

– La couche liaison, niveau trame ou X.25-2, met en œuvre un sous-ensemble d'HDLC appelé LAP-B (*High Level Data Link Control, Link Access Protocol Balenced*).

– La couche réseau, niveau paquet ou X.25-3, gère les circuits virtuels (permanents ou commutés). Si un ETTD peut communiquer simultanément, sur une même liaison d'abonné, avec plusieurs sites distants, l'accès au réseau est dit multivoie, dans le cas contraire, l'accès est dit **univoie** ou **monovoie**.

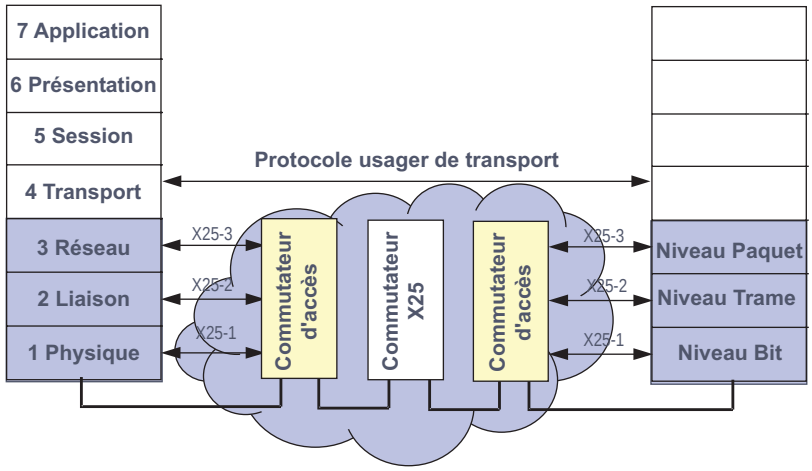


Figure 11.24 Architecture du protocole X.25.

Rappelons que X.25 ne concerne que l'accès au réseau. Le réseau de transport peut utiliser, dans le réseau interne, un protocole différent.

Le niveau X.25-1

La recommandation X.25 spécifie que l'accès au réseau X.25 doit être conforme à l'une des recommandations X.21 (transmission numérique), X.21 bis (transmission analogique) ou X.31 (accès via le RNIS). L'avis X.21 définit l'interface d'accès entre un ETTD et un réseau public de transmission de données (figure 11.25), il fixe les règles d'échange pour :

– L'établissement de la connexion avec un ETTD distant à travers un ou plusieurs réseaux.

– L'échange des données en mode duplex intégral.

– La libération de la connexion.

Ces interfaces sont étudiées à la section 5.4.2, le lecteur pourra utilement s'y reporter.

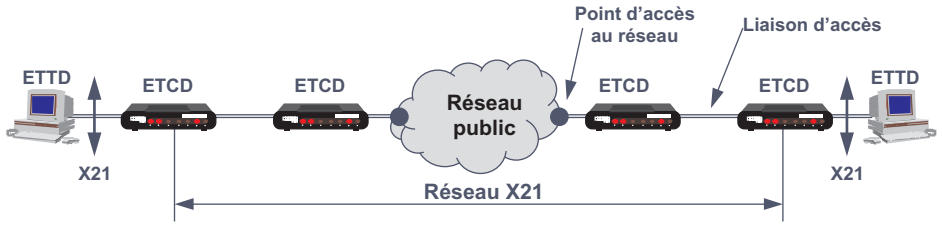


Figure 11.25 Le réseau X.21.

Le niveau X.25-2

➤ Généralités[7]

Le niveau 2 du modèle OSI, ou couche liaison, garantit un transfert fiable de données sur une liaison physique non fiable (perturbations électromagnétiques). Au niveau trame, X.25-2 met en œuvre le protocole HDLC LAP-B (*Link Access Protocol Balanced*). LAP-B est un protocole point à point en duplex intégral (*full duplex*), dans lequel les deux stations communicantes ont une responsabilité égale vis-à-vis de la liaison, chacune des extrémités pouvant émettre une commande. L'une des stations est l'ETTD (DTE), l'autre le nœud de rattachement au réseau ou ETCD (DCE) (en X.25, le réseau ou son point d'accès est assimilé au DCE). La figure 11.26 schématise le principe d'une liaison équilibrée.

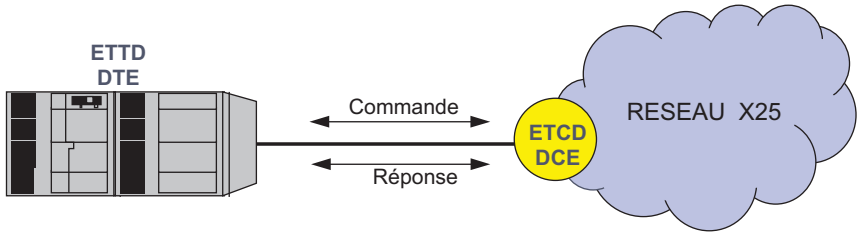


Figure 11.26 Liaison point à point en LAP-B.

L'accès au réseau peut utiliser un seul lien physique (**SLP**, *Simple Link Pro*tocol) ou, pour accroître le débit, une agrégation de plusieurs liens (**MLP**, *Multi Link Protocol*). L'utilisation de MLP est transparente pour le niveau réseau, avec l'évolution des débits l'utilisation du protocole MLP est tombée en désuétude.

➤ HDLC LAP-B versus SLP

La procédure HDLC LAP-B, étudiée section 6.5, utilise deux modes de fonctionnement : le fonctionnement normal (numérotation des trames sur 3 bits, modulo 8) et le mode étendu (numérotation des trames sur 7 bits, modulo 128). La structure générale de la trame HDLC est rappelée figure 11.27

HDLC utilise trois types de trames :

– Les trames d'information (**I**) contiennent un champ de données. Les champs $N_{(s)}$ et $N_{(r)}$ correspondent, pour chaque extrémité de la liaison, à un compteur de trames d'information émises $V_{(s)}$ ou reçues $V_{(r)}$.

7. Le protocole HDLC est étudié en détail au chapitre 6, *Notions de protocole*.

© Dunod – La photocopie non autorisée est un délit

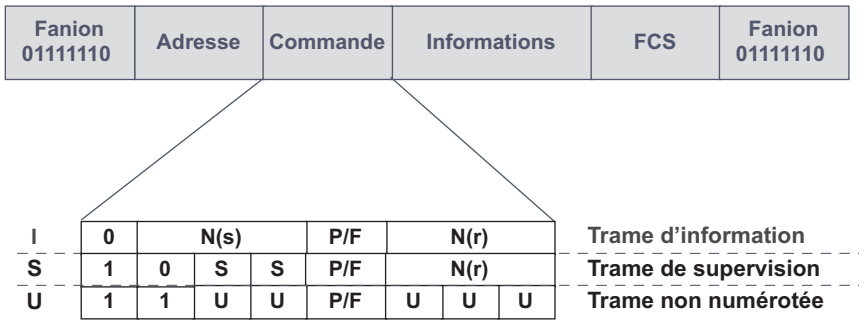

Fanion 01111110
Adresse
Commande
Informations
FCS
Fanion 01111110
I 0 N(s) P/F N(r) Trame d'information
S 1 0 S S P/F N(r) Trame de supervision
U 1 1 U U P/F U U U Trame non numérotée

Figure 11.27 Rappel sur la structure de la trame HDLC.

– Les trames de supervision (**S**) permettent de contrôler l'échange de données. Le champ $N_{(r)}$ identifie la trame acceptée ou refusée ($N_r - 1$), il correspond au $N_{(s)}$ de la prochaine trame attendue.
– Les trames non numérotées (**U**, *unnumbered*) gèrent la liaison (établissement, libération...). Elles ne comportent aucun compteur (non numérotées).

Le contrôle et la reprise sur erreur sont réalisés entre chaque nœud du réseau. Notons que pour se prémunir contre la perte d'un fanion, le calcul du FCS (*Frame Check Sequence*) est le complément à 1 de la division polynomiale du contenu de la trame par le polynôme générateur $G_{(x)} = x^{16} + x^{12} + x^5 + 1$ (avis V41 de l'UIT-T). En émission, le registre de calcul du FCS est initialisé à 1, dans ce cas, en réception, le reste de la division est toujours 0001110100001111. Ce nombre est dit **nombre magique**.

Pour ouvrir une connexion (figure 11.28), l'ETCD ou ETTD appelant émet une trame non numérotée (trame U) SABM (ouverture en mode normal) ou SABME (ouverture en mode étendu). L'appelé l'acquitte avec la trame non numérotée UA. Sans réponse de l'appelé, l'appelant à échéance d'un *timer* (**T1**) renouvelle sa demande. Il abandonne la demande d'établissement après **N2** tentatives infructueuses, en principe le compteur N2 est initialisé à 10, il est décrémenté de 1 à chaque tentative.

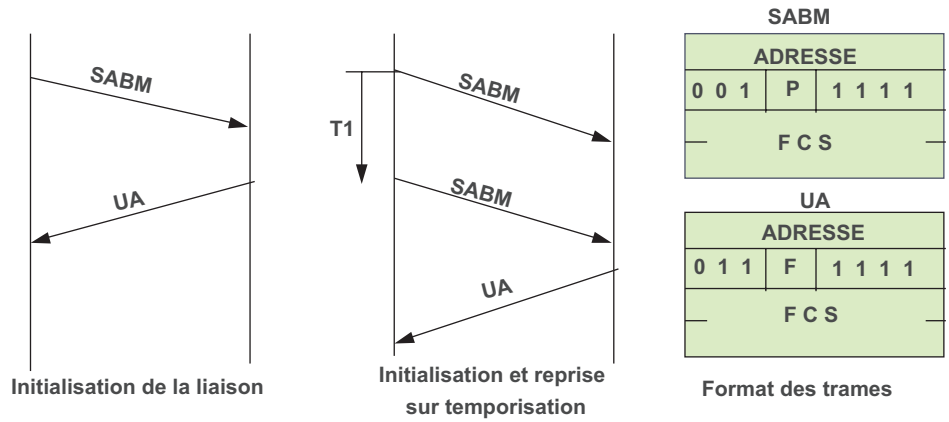


Figure 11.28 Ouverture de connexion.

Lorsque la connexion est acceptée, l'appelant ou/et l'appelé peut(vent) procéder à l'échange d'information (trames I), cet échange est contrôlé par des trames de supervision (trames S).

Les trames d'information ($N_{(s)}$) sont numérotées modulo 8 (mode de base) ou modulo 128 (mode étendu). La gestion de la fenêtre (la taille de la fenêtre niveau liaison est définie à l'abonnement) permet l'anticipation de l'émission par rapport aux accusés de réception.

L'accusé de réception (figure 11.29) peut être explicite par une trame RR. Le récepteur n'a alors pas d'information à transmettre. Le compteur $N_{(r)}$ indique donc le numéro $N_{(s)}$ de la prochaine trame attendue. Dans l'acquittement implicite ce sont les trames d'information du correspondant distant (échange *full duplex*) qui effectuent l'acquittement (compteur $N_{(r)}$ des trames I).

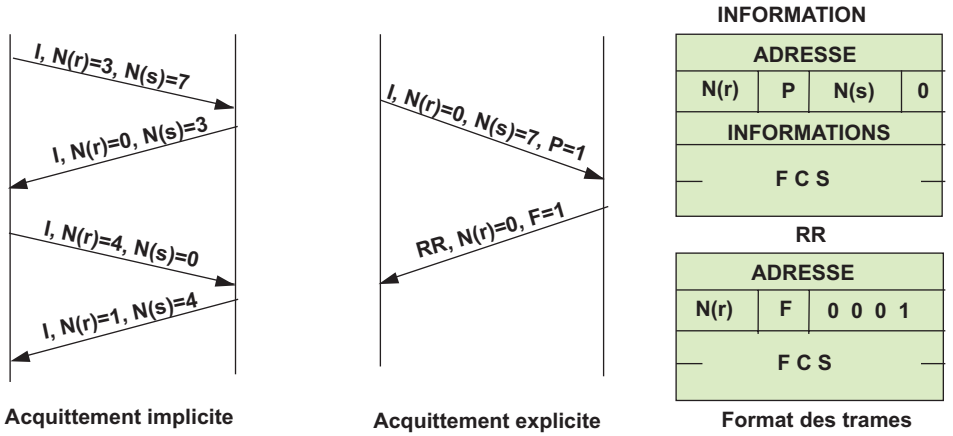


Figure 11.29 Transfert de données.

Les trames S, RR, REJ et RNR supervisent l'échange. La trame RR sert à l'acquittement, la trame REJ indique la trame rejetée (trame erronée ou numéro de séquence invalide) et demande de reprendre la transmission depuis la trame erronée (compteur N_r). La trame RNR acquitte la trame N_r-1 et demande à l'émetteur d'arrêter provisoirement son émission. Le récepteur signale ainsi qu'il n'est pas en état de recevoir d'autres trames, c'est le mécanisme du contrôle de flux (état bloqué ou occupé), les émissions reprendront à réception d'une trame RR ou REJ (figure 11.30). La trame SREJ (rejet sélectif) ne demande la retransmission que de la trame rejetée.

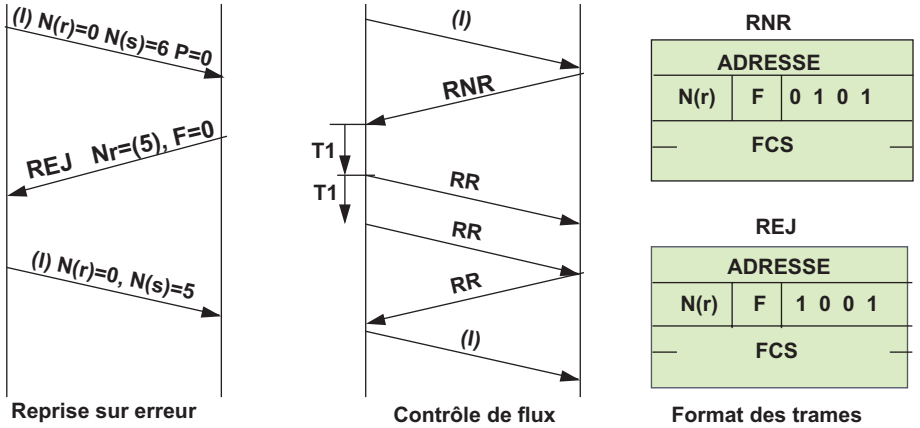


Figure 11.30 Reprise sur erreurs et contrôle de flux.

© Dunod – La photocopie non autorisée est un délit

La déconnexion est demandée par l'ETTD ou ETCD par la trame DISC ; à la réception d'une demande de déconnexion, le destinataire émet un acquittement de celle-ci (UA) et se déconnecte. L'émetteur de la demande de déconnexion n'exécute la procédure de déconnexion qu'après avoir reçu l'acquittement de sa demande.

Toutes les trames d'information non acquittées sont ignorées. La procédure de déconnexion est représentée figure 11.31. le réseau (ETCD) peut signaler un incident de ligne (modem coupé par exemple) par l'émission de trames DM. Après **N2** retransmissions, il passe à l'état déconnecté.

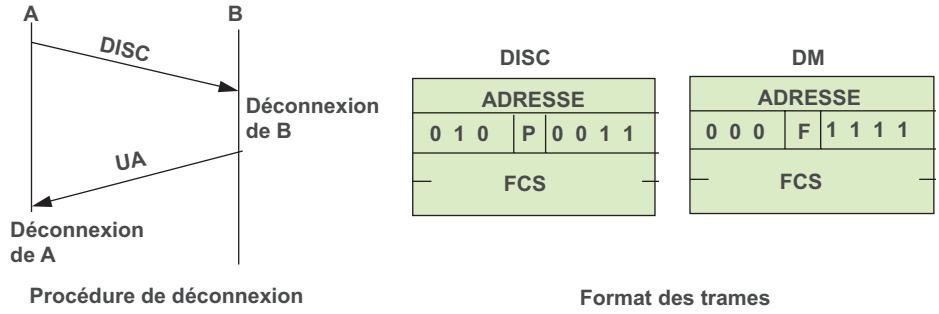


Figure 11.31 Rupture de la liaison.

Lorsque les erreurs ne peuvent être corrigées par une simple retransmission de la ou des trames litigieuses (nombre de retransmissions supérieur à N2, $N_{(r)}$ incorrect : valeur supérieure au nombre de trames réelles...), l'ETCD ou ETTD peut effectuer une déconnexion (DISC) ou réinitialiser la liaison (SABM). Certaines erreurs sont signalées avant la réinitialisation de la liaison par la trame FRMR (figure 11.32). Les variables d'états $V_{(s)}$ et $V_{(r)}$ indiquent alors au destinataire l'état des compteurs de son correspondant. Le bit C/R à 1 indique que la trame rejetée est une réponse, à 0 que la trame rejetée est une commande.

ADRESSE
1 0 0 F 0 1 1 1
0 0 0 0 Z Y X W
Champ commande de la trame reçue
V(r) C/R V(s) 0
FCS
Codage des bits
Z Y X W
Signification
0 0 0 1 Le champ commande de la trame reçue est incorrect
0 0 1 1 La longueur du champ information est incorrecte
1 0 0 0 La valeur de N(r) est incorrecte
0 1 0 0 La taille du champ d'information est excessive

Figure 11.32 Trame d'indication d'erreurs FRMR.

Le niveau X.25-3

➤ Généralités

La recommandation X.25-3 (**X.25 PLP**, *Packet Level Protocol*) gère l'établissement, le maintien et la libération des circuits virtuels (**CVC**, Circuit Virtuel Commuté ou **SVC**, *Switched*

Virtual Circuit). Elle résout les problèmes d'adressage et de multiplexage des connexions virtuelles sur la même liaison d'abonné. Le protocole X.25-3 assure le transfert de données, le contrôle de flux, la fragmentation et le réassemblage des paquets.

La procédure d'établissement des CVC établit une relation entre un numéro de voie entrante d'une part et le numéro de voie sortante d'autre part. Cette relation correspond à un lien virtuel entre les entités connectées (connexion virtuelle) similaire à la constitution d'un circuit en commutation de circuits. Le mode de mise en relation est dit orienté connexion. Ce procédé (figure 11.33) qui identifie une liaison, autorise le multiplexage des connexions sur une même voie physique et l'utilisation d'un adressage abrégé : le Numéro de Voie Logique (**NVL**).

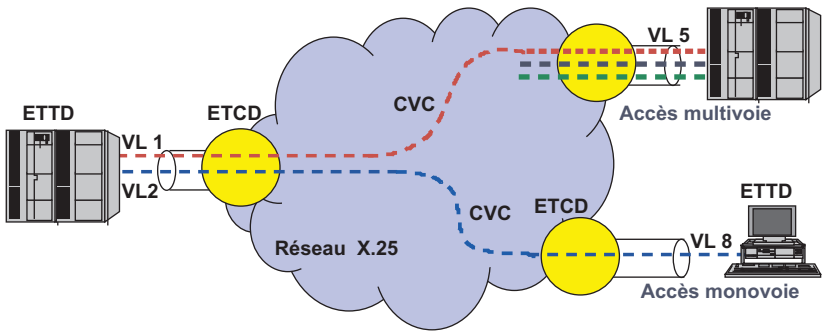


Figure 11.33 Mise en relation d'abonnés.

➤ Format des unités de données

Les paquets X.25-3 comportent les informations relatives à l'adressage : le numéro de voie logique utilisée (adressage de convention), des informations de contrôle et éventuellement des données. Les paquets sont transmis à la couche trame qui les encapsule (figure 11.34).

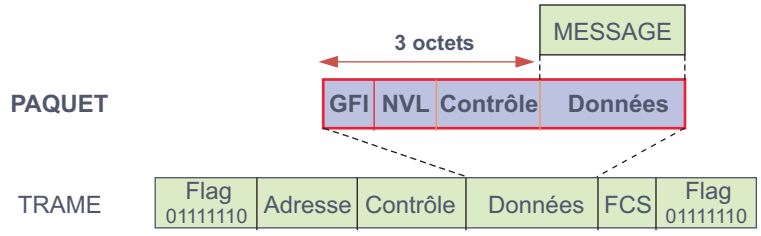


Figure 11.34 Encapsulation des paquets X.25 dans les trames LAPB.

Un paquet X.25, illustré figure 11.35, comporte au moins 3 octets. Le premier champ de 4 bits, dit champ **GFI** (*General Format Identifier*) définit certains paramètres de l'échange. Le premier bit a deux significations. Dans les paquets de données il est dit bit **Q** (*Qualified*), dans les paquets d'établissement bit **A** (*Address*). Le bit Q (bit à 1) est, par exemple, utilisé pour indiquer au PAD (accès asynchrone à X.25) que le paquet est une commande à son intention et non un paquet de données à transmettre à ETTD. Le bit A, dans les paquets d'établissement (ou d'appel) identifie le format du champ adresse. Si le bit A est à 0, l'adresse est au format X.121, sinon le format de l'adresse est indiqué dans le champ adresse. Le bit **D** (*Delivery*) détermine la portée des acquittements. Si le bit D est à 1 l'acquittement a une signification de bout en

© Dunod – La photocopie non autorisée est un délit

bout, sinon il est local. La recommandation X.25, antérieure au modèle OSI, n'est, sur ce point pas conforme aux spécifications du modèle de référence qui ne prévoit un acquittement de bout en bout qu'au niveau de la couche transport. Les deux bits suivants indiquent la taille des compteurs (01, modulo 8 ; 10, modulo 128).

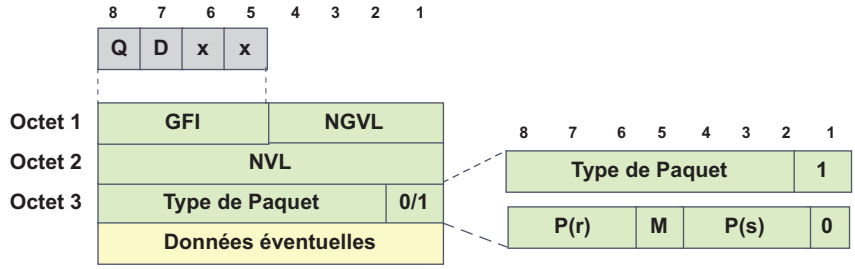


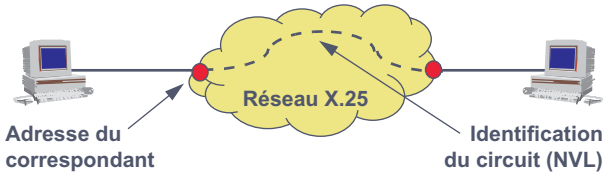
Figure 11.35 Format des paquets X.25.

Le champ suivant identifie la voie logique (étiquette) : le **NVL** ou Numéro de Voie Logique sur 12 bits (4 096 voies logiques identifiables) n'a qu'une signification locale. Le NVL est composé de 2 champs, les 4 premiers bits de l'octet 1 identifient le groupe de voies logiques (NGVL) auquel appartient la voie logique (octet 2).

Enfin, le dernier champ de l'en-tête correspond au champ commande d'HDLC. Le premier bit différencie un paquet de données (bit à 0) des autres types de paquets (bit à 1). Dans les paquets de données les champs $P_{(r)}$ et $P_{(s)}$ (sur 3 bits en mode normal) permettent de contrôler le séquencement des paquets. Ces compteurs ne font pas double usage avec ceux du niveau trame. En effet, une connexion de niveau 2 peut multiplexer plusieurs connexions de niveau 3. Enfin, le bit **M** (*More data*) est utilisé lorsque le paquet transmis a subi une fragmentation. M = 1 signifie que les paquets qui suivent appartiennent au même bloc de données. M = 0 identifie le dernier paquet ou un paquet non fragmenté.

➤ Gestion des circuits virtuels

Les réseaux X.25 autorisent les deux types de circuits virtuels, les circuits virtuels commutés (CVC ou SVC) et les circuits virtuels permanents (CVP ou PVC, *Permanent Virtual Circuit*). La figure 11.36 rappelle les différences essentielles entre ces deux modes de mises en relation.



	Circuit Virtuel Commuté	Circuit Virtuel Permanent
Etablissement du circuit	A chaque appel	A l'abonnement
Potentialité de communication	Possibilité de mise en relation avec tout abonné	Liaison point à point
Temps d'établissement	Peut être long (1s)	Sans (Liaison permanente)

Figure 11.36 Différences entre un CVC et un CVP.

Le circuit virtuel permanent est établi par l'opérateur à la configuration du raccordement de l'abonné. À l'inverse, le circuit virtuel commuté est construit appel par appel. Les identifiants de voie (NVL) sont attribués dynamiquement par chaque nœud (terminal utilisateur ou nœud du réseau). Le numéro affecté est choisi parmi ceux disponibles qui sont gérés par une table interne au nœud. Ce procédé peut conduire à une collision d'appels, c'est-à-dire à une affectation simultanée d'un même NVL à un appel sortant et à un appel entrant. En cas de collision d'appels, l'ETTD ignore l'appel entrant, l'ETCD (le réseau) traite l'appel en provenance de l'ETTD local et entame une procédure de déconnexion pour l'appel de l'ETTD distant (figure 11.37).

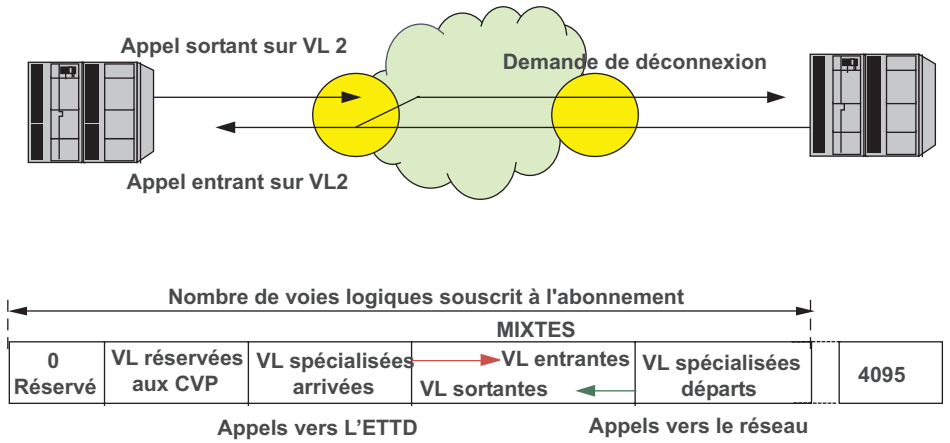


Figure 11.37 Gestion des numéros de voies logiques.

Pour minimiser le risque de collision d'appels, les appels sortants de l'ETTD sont émis sur la voie logique de numéro le plus élevé. Le réseau transmet les appels entrants sur le numéro de voie logique disponible le plus faible. Comme en téléphonie, il est possible de définir les voies logiques en voies logiques spécialisées arrivées ou départs. Une voie qui accepte aussi bien les arrivées que les départs est dite **mixte**. L'affectation des NVL s'effectue comme le montre le diagramme de la figure 11.37. Les premiers numéros de voies logiques sont réservés aux circuits virtuels permanents. La voie logique 0 est en principe réservée à l'opérateur pour la signalisation d'incidents.

➤ Adressage des ETTD distants

Durant la procédure d'établissement et de la libération du CV, les ETTD sont identifiés par leur numéro réseau (adresse d'abonné). Les champs adresse des paquets d'établissement sont codés en Décimal Codé Binaire (**DCB**) sur un quartet. Un champ longueur d'adresse précède celle-ci. La recommandation X.25 admet deux types d'adresse. Implicitement, l'adressage est conforme à la recommandation X.121 (voir section 8.3.2).

➤ Facilités ou services complémentaires

Les paramètres de la liaison sont généralement fixés au moment du raccordement (abonnement), cependant certains peuvent être négociés ou renégociés appel par appel. Les facilités ou services complémentaires sont invoqués dans le paquet d'appel (ou paquet d'établissement).

© Dunod – La photocopie non autorisée est un délit

Le champ option est codé : code option et paramètres de l'option. Le tableau de la figure 11.38 fournit quelques exemples d'options.

Option	Code option	Codage	Description
Groupe fermé d'abonnés	0x03	DCB, 1 chiffre par quartet	Le GFA permet de constituer un réseau privé dans le réseau public. Seuls peuvent communiquer les hôtes appartenant au même GFA.
Taxation au demandé	0x01	0x01 (taxation demandée)	Elle permet de centraliser la facturation sur un même site (réduction quantitative).
Sélection rapide	0x01	0x80	Elle permet de joindre à un paquet d'appels jusqu'à 128 octets de données (même code que la taxation au demandé).
Classe de débit	0x02	1er quartet vers DTE 2e quartet du DTE Ex de valeurs : 3 75 bit/s 7 1 200 bit/s B 19 200 bit/s C 48 000 bit/s D 64 000 bit/s	Elle est utilisée pour adapter le débit de l'hôte aux capacités de réception du destinataire sans avoir besoin de recourir au contrôle de flux.
Taille des paquets	0x42	Taille en émission sur 1 octet Taille en réception sur 1 octet Exprimée en puissance de 2 de la taille Ex : 128 codée 7	Selon les ETCD, la taille en émission et en réception peut être différente.
Taille des fenêtres	0x43	Taille en émission 1 octet Taille en réception 1 octet	Selon les ETCD.

Figure 11.38 Exemples d'options X.25.

➤ Établissement et libération des circuits virtuels

L'ETTD qui prend l'initiative d'établir une connexion émet une demande d'appel (paquet d'appel), le paquet d'appel sortant est émis sur la première voie logique disponible. Le paquet d'appel contient toutes les informations nécessaires à l'établissement du CV (figure 11.39), c'est-à-dire :

– L'étiquette affectée (**NVL**, Numéro de Voie Logique).

– L'adresse complète.

– Si des facilités sont demandées, la liste des facilités invoquées est précédée de la longueur totale du champ facilités, sinon l'octet longueur du champ facilités est à zéro.

– Enfin, suivent des données utilisateur sur 16 octets ou 128 si la facilité **sélection rapide** a été demandée.

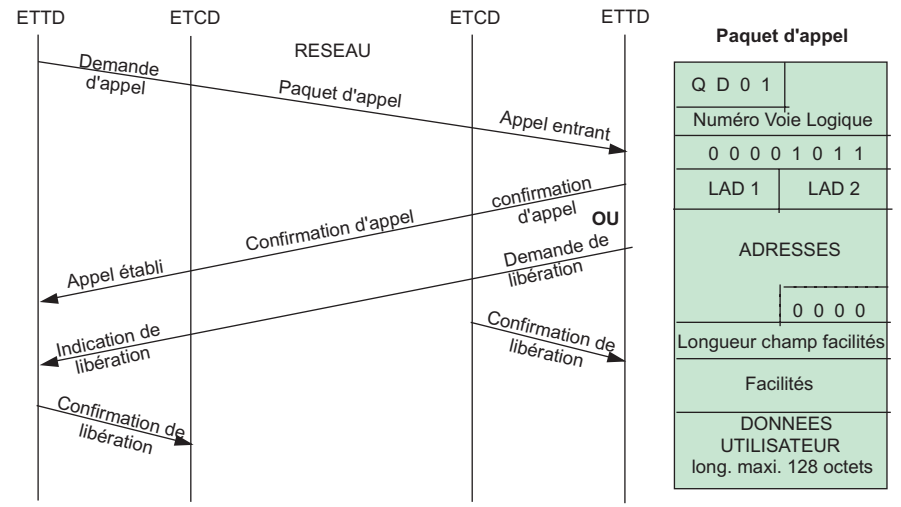


Figure 11.39 Diagramme d'établissement d'appel. (LAD1 Longueur adresse appelant, LAD2 Longueur adresse appelé)

Le réseau transmet alors à l'appelé un appel entrant, le champ facilité peut, éventuellement, en fonction des options offertes par le réseau de raccordement, avoir été modifié par ce dernier. Le circuit virtuel est alors établi.

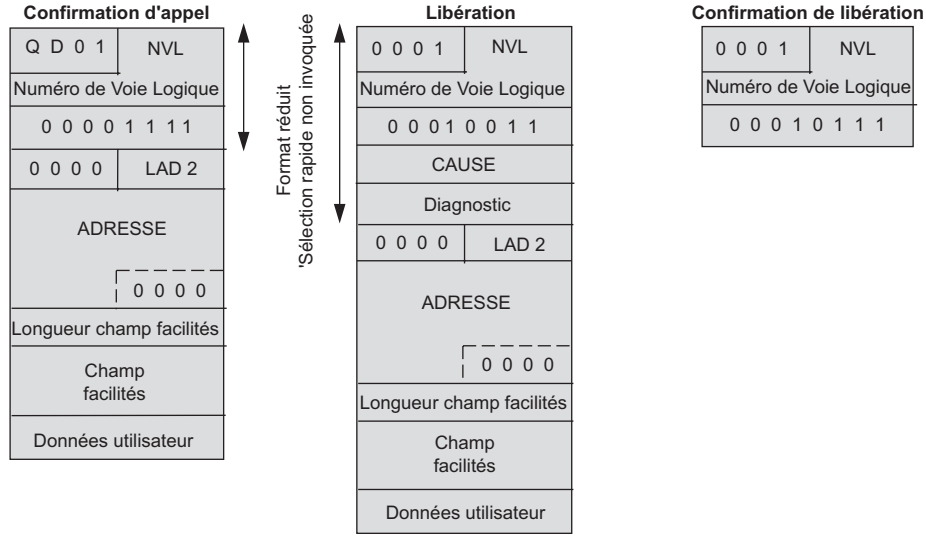


Figure 11.40 Format des paquets de confirmation et libération.

L'appelé peut accepter (paquet de confirmation d'appel, figure 11.40) ou refuser l'appel (paquet de libération). Un paquet de confirmation de libération confirme à l'ETTD ou ETCD que le CV a bien été libéré. La libération d'un circuit virtuel peut être provoquée par le réseau suite à un refus d'appel (appelé occupé, refus de la taxation au demandé, GFA non accepté...) ou à un incident interne au réseau. L'ETTD qui désire mettre fin à un échange (fin de connexion) émet un paquet de demande de libération (figure 11.40).

© Dunod – La photocopie non autorisée est un délit

➤ Échange de données

Chaque circuit virtuel établi peut supporter un transfert de données bidirectionnel limité, en débit, par le paramètre **classe de débit**. La figure 11.41 illustre les paquets utilisés lors d'un échange de données.

Figure 11.41 Format des paquets de données, d'acquittement et de contrôle de flux.

La taille du champ de données est définie à l'abonnement ou par l'opérateur, cette taille est fixée par la norme X.25 à 16, 32, 64, 128, 256, 512, 1024, 2 048 ou 4 096 octets. L'échange de données s'effectue selon un mécanisme similaire à celui étudié pour HDLC. Les compteurs $P_{(s)}$ et $P_{(r)}$ des paquets de données permettent de vérifier le séquencement des paquets (perte éventuelle d'un paquet) et d'acquitter ceux-ci ($P_{(r)}$, numéro du paquet attendu). Les paquets **RR** (*Receive Ready*) et **RNR** (*Receive Not Ready*), (figure 11.41) assurent l'acquittement et le contrôle de flux.

➤ Gestion des incidents

Lorsque le réseau, ou l'un des ETTD, détecte une désynchronisation des échanges (Numéros $P_{(s)}$, et $P_{(r)}$, il demande une réinitialisation des compteurs par l'émission d'un paquet de demande de réinitialisation. Les données en cours de transfert sont abandonnées, les compteurs sont remis à zéro. La demande de réinitialisation ne concerne que le CV sur lequel elle a été émise. Le mécanisme de la réinitialisation est illustré par la figure 11.42.

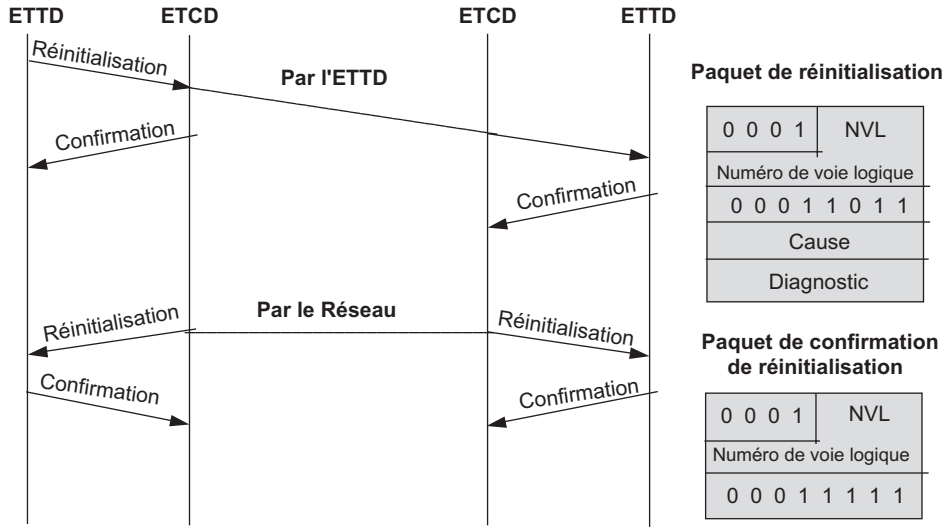


Figure 11.42 Mécanisme de la réinitialisation.

Le mécanisme de reprise ou de redémarrage est déclenché suite à un incident grave sur le réseau (rupture de la liaison physique...). Il affecte tous les circuits virtuels établis et les circuits virtuels permanents. Les CVC établis sont libérés, les CVP actifs sont remis à l'état initial. Le mécanisme de la reprise est représenté figure 11.43.

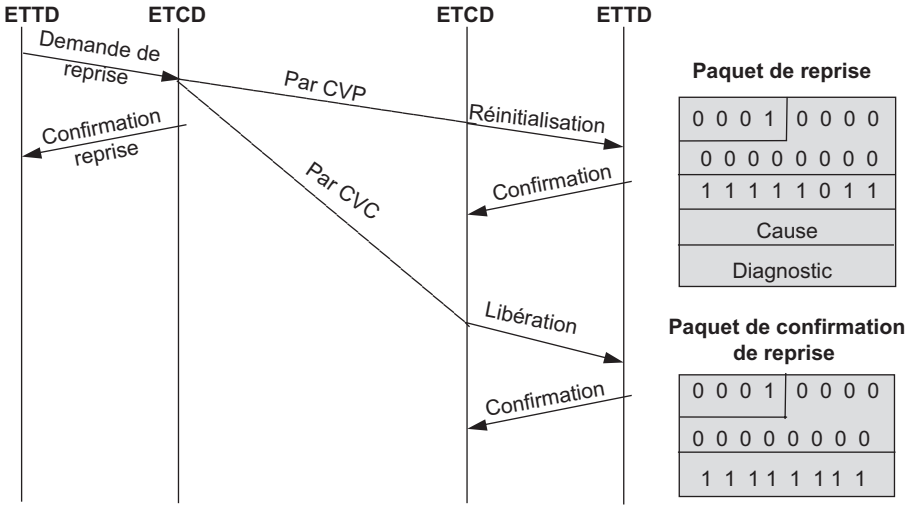


Figure 11.43 Mécanisme de la reprise.

Les paquets de demande de reprise et d'indication de reprise sont émis sur la voie logique 0. Le champ cause indique la raison de la reprise, le champ diagnostic complète cette information. Le tableau de la figure 11.44 fournit quelques exemples de codage des champs cause et diagnostic des paquets de reprise et de diagnostic

Cause	Signification	Diag.	Signification
Reprise		24	Numéro de VL inexistant
01	Erreur de procédure locale	26	Paquet trop court
07	Fin d'incident	27	Paquet trop long
Réinitialisation		28	Erreur de codage du champ GFI
00	Par l'abonné distant	52	Longueur non-multiple de 8
01	Dérangement de l'abonné distant	97	Modem abonné hors tension
03	Erreur de procédure locale	A1	Bit F reçu à tort
07	Incident dans le réseau	A4	Non-réponse à N2
09	Fin de dérangement	A9	Trop d'erreur de ligne

Figure 11.44 Exemples de cause et de diagnostic d'erreur.

Attention : la réinitialisation ne concerne que le CV sur lequel elle a été émise. La reprise concerne tous les CV y compris les CVP, elle est émise sur le CV 0.

➤ L'accès des terminaux asynchrones aux réseaux X.25

La norme X.25 définit un protocole pour l'accès en mode paquets de terminaux synchrones (**ETTD-P**). Les terminaux asynchrones (ou terminaux en mode caractères : **ETTD-C**, par exemple les terminaux TTY ou ceux de la série VT100...) nécessitent une adaptation pour converser à travers un réseau en mode paquets. Une fonction de groupage, ou conversion des

© Dunod – La photocopie non autorisée est un délit

caractères émis en paquets et la fonction inverse de dégroupage des paquets en caractères, doit être interposée entre le terminal et le réseau. Les fonctions d'assemblage et de désassemblage des paquets sont effectuées au point d'accès du réseau par un organe appelé : **PAD** (*Packet Assembler Disassembler*). Les recommandations X.28, X.29, X.3 régissent ce type d'accès, X.28 définit le dialogue en mode caractères entre le terminal et le PAD, X.3 précise le fonctionnement du PAD et X.29 décrit le dialogue de commande entre l'ETTD-P et le PAD, cette organisation est symbolisée par la figure 11.45.

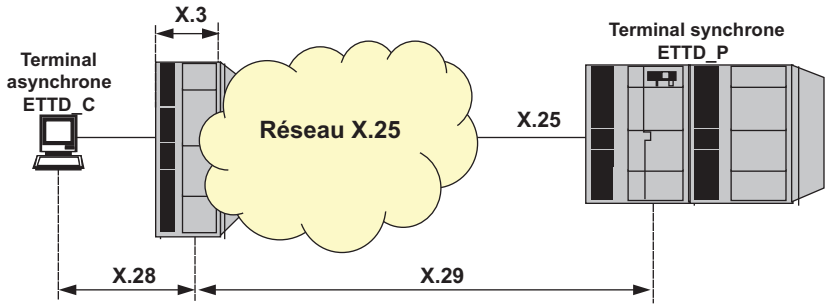


Figure 11.45 Accès des ETTD-C aux réseaux X.25.

Les fonctions du PAD (X.3)

La fonction PAD a pour objectif essentiel d'encapsuler les données issues du terminal asynchrone dans un paquet X.25 et de désencapsuler les données à destination de ce terminal. Afin d'éviter que sur le réseau ne circule un paquet pour chaque caractère, le PAD assemble ces caractères en paquets, l'avis X3 précise les modalités essentielles de cette fonction :

– Il définit le nombre de caractères que le PAD devra avoir reçus avant d'émettre un paquet sur le réseau.

– Il précise les caractères de commande qui déclenchent l'émission d'un paquet même incomplet (retour chariot RC, BREAK...).

– Il détermine le temps maximum d'attente entre deux caractères avant d'envoyer un paquet (émission sur temporisation).

D'autres fonctions relatives à la transmission ou à la gestion du terminal peuvent être remplies. Ce sont notamment :

– L'écho local, sur un terminal asynchrone : l'affichage du caractère sur l'écran n'est pas celui introduit au clavier mais celui renvoyé en écho par l'ETTD distant (fonction de correction d'erreur par l'opérateur). Pour éviter un trafic inutile sur le réseau, l'écho du caractère introduit peut-être généré par le PAD (écho local). La fonction d'écho peut être annulée lors de l'introduction d'un mot de passe (frappe en aveugle).

– Le pliage de ligne : c'est un paramètre qui permet d'adapter la longueur des messages reçus aux possibilités d'affichage du terminal (nombre de caractères/ligne), le PAD introduit les caractères CR/LF après *n* caractères.

– Le contrôle de flux par emploi d'une procédure XON, XOFF.

Le dialogue ETTD-C/PAD (X.28)

X.28 définit l'interface physique, la procédure d'établissement du circuit virtuel et l'accès du terminal aux paramètres du PAD (Lecture et modification). L'accès d'un terminal caractère à un réseau X.25 utilise des communications asynchrones d'un débit allant de 1 200 à 14 400 bit/s répondant aux avis V.22 et V.22bis.

Le niveau bit est considéré établi entre le PAD et ETTD-C par détection de réception de porteuse pendant plus de 20 s. L'échange de caractères peut alors commencer. La figure 11.46 représente le scénario d'établissement d'une liaison entre un ETTD-C et un ETTD-P à travers un réseau X.25. Le terminal reçoit une indication de connexion (par exemple le mot TRANSPAC), il répond en donnant le numéro de l'abonné demandé, l'établissement du CV est concrétisé par le message COM, le refus d'établissement par la réception du mot LIB éventuellement suivi d'un code d'erreur (LIB ERR).

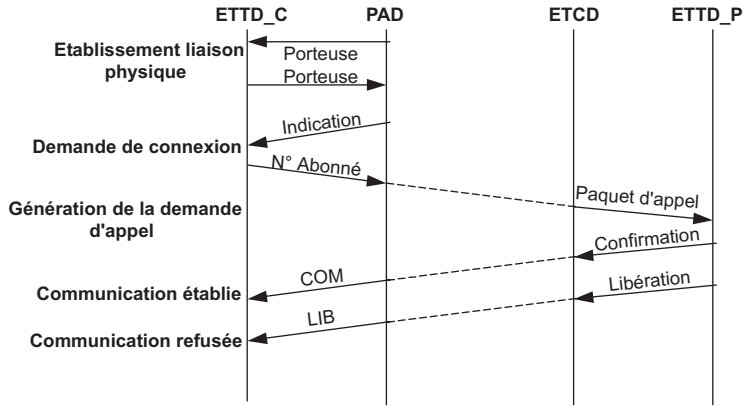


Figure 11.46 Établissement d'un CV via un accès asynchrone.

Le dialogue ETTD-P/PAD (X.29)

X.29 décrit les procédures que l'ETTD-P peut utiliser pour contrôler le fonctionnement du PAD. L'ETTD-P adresse au PAD des messages de commande PAD, ce dernier y répond par des messages PAD d'indication. Les messages de commande et d'indication sont véhiculés par des paquets avec le bit Q à 1.

➤ Les accès aux réseaux X.25

Généralités

Toutes les applications ne nécessitent pas un accès permanent au réseau, de ce fait, une liaison permanente peut s'avérer coûteuse en regard de son taux d'utilisation. C'est pour ces raisons qu'ont été définis des accès temporaires via le réseau téléphonique. La diversité des modes d'accès constitue l'un des facteurs de pérennité de ce protocole.

X.25 distingue deux types d'accès : les accès permanents ou accès directs établis via une liaison spécialisée ou le canal D de RNIS et les accès commutés ou accès indirects qui transitent via le RTC ou RNIS (canal B). La figure 11.47 représente ces deux types d'accès.

© Dunod – La photocopie non autorisée est un délit

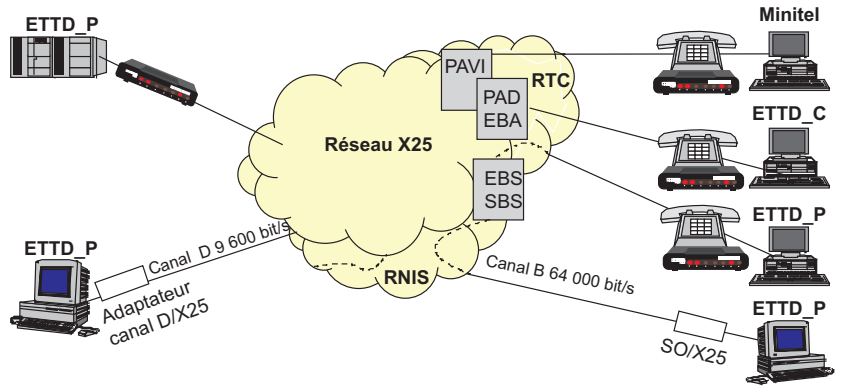


Figure 11.47 Les accès au réseau X.25.

Les accès directs

La liaison spécialisée constitue l'accès normal au réseau X.25. Un lien dépendant du débit de l'abonnement est établi de manière permanente entre le commutateur de rattachement de l'abonné et ce dernier. Généralement, les éléments d'interconnexion sont fournis par l'opérateur. Ce type de raccordement est mal adapté à un besoin de connexion permanente avec un faible échange de données (taux de connexion important, taux d'activité faible). Le canal D des réseaux RNIS offre un accès permanent à 9 600 bit/s mieux adapté à ce cas de figure.

Les accès indirects

Les accès indirects (mode paquets ou caractères) transitent par un réseau intermédiaire (RTC ou RNIS) et convergent vers un point d'accès ou porte spécialisée selon le type d'accès (PAD, PAVI, EBS...). Un service d'identifiant peut être souscrit à l'abonnement. Les accès indirects sont essentiellement utilisés pour :

– des consultations de faible ou moyenne durée (Minitel ou autre) ;

– des transferts de petits fichiers ;

– des raccordements de secours pour des accès directs.

Conclusion

La décentralisation des traitements vers une architecture largement distribuée de type client/serveur a modifié l'amplitude et la nature des trafics sur les liens d'interconnexion. L'accroissement des débits nécessaires et la sporadicité des échanges caractérisent essentiellement cette évolution, rendant obsolète les offres de débit figées telles que celles d'X.25.

Le développement d'applications multimédias (données, son, vidéo) a, non seulement, engendré un besoin de débit plus important, mais a introduit également des contraintes temporelles strictes dans les échanges (trafic isochrone). X.25 ne peut répondre à cette demande.

La limitation du débit des réseaux X.25 résulte principalement du temps de traversée du réseau en raison essentiellement des traitements dans les différents nœuds et non à cause du débit des lignes. Étudié pour assurer une certaine qualité de service sur des supports peu fiables (supports cuivre ou hertzien), X.25 génère un grand nombre d'opérations de couche, redon-

dantes d'une couche à l'autre, qui pénalisent gravement le débit effectif (**TTI**, Taux de Transfert des Informations) :

– La détection et la reprise sur erreur en point à point (couche 2), alors que les réseaux tout optique ont considérablement abaissé le taux d'erreur.
– La gestion des fenêtres et l'acquittement de nœud à nœud (couche 2 et couche 3).
– Le contrôle de flux (couche 2 et 3) ;
– Le routage (paquet d'appel) et la commutation (paquet de données) qui s'effectuent au niveau 3.

Ce n'est que par une réponse architecturale différente que ces nouvelles exigences et contraintes seront résolues.

11.2.3 Évolution vers les hauts débits

L'augmentation du débit réel ne peut résulter que de l'allégement des traitements intermédiaires, ce qui a conduit à :

– reporter sur les organes d'extrémité (les calculateurs) les tâches de détection et de reprise sur erreur ;
– diminuer les opérations de couches en effectuant les opérations d'acheminement le plus bas possible, sans avoir à remonter au niveau 3 ;
– formuler des hypothèses optimistes sur le comportement du réseau en n'effectuant pas de contrôle de flux entre les nœuds ;
– supprimer les acquittements intermédiaires, ceux-ci n'étant réalisés que par les organes d'extrémité (acquittement de bout en bout) ;
– simplifier le traitement dans les nœuds en n'utilisant qu'un seul type de données et en mettant en œuvre une signalisation par **canal sémaphore** pour l'établissement des circuits et la gestion du réseau.

C'est l'introduction de la fibre optique qui en fiabilisant la transmission a autorisé cette simplification des protocoles. La figure 11.48 représente l'architecture générale de ces nouveaux protocoles.

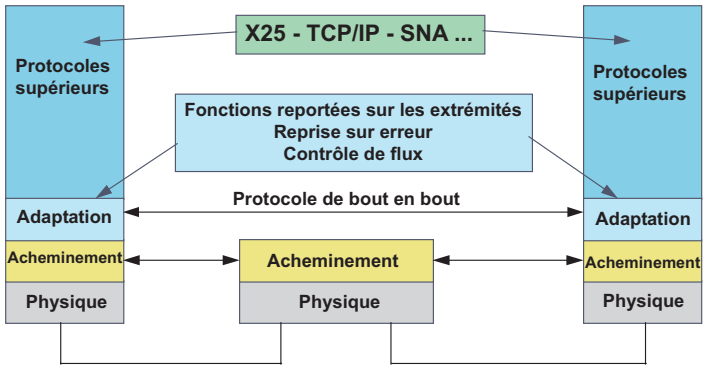


Figure 11.48 Architecture générale des réseaux haut débit.

© Dunod – La photocopie non autorisée est un délit

La couche 2 est scindée en deux sous-couches : un noyau assurant les fonctions élémentaires d'acheminement, de détection d'erreur et de signalisation de la congestion, et une couche d'adaptation entre les protocoles supérieurs et le noyau. Cette dernière, facultative, n'est présente que sur les organes d'extrémité. L'ensemble assure la transparence aux protocoles supérieurs.

Les protocoles hauts débits se sont développés selon deux approches (figure 11.49) :

– Le relais de trames ou *Frame Relay* qui correspond à un allégement du protocole HDLC LAP-D. Ce protocole répond aux besoins de haut débit mais, comme à l'origine il ne traitait pas les flux isochrones, il a généralement été perçu comme un protocole de transition entre X.25 et ATM ;

– Le relais de cellules ou *Cell Relay*, plus connu sous le nom **d'ATM** (*Asynchronous Transfer Mode*) qui utilise une technique de commutation rapide de cellules de taille fixe. ATM met en œuvre des mécanismes spécifiques pour assurer les transferts isochrones (émulation de circuits pour la voix et la vidéo).

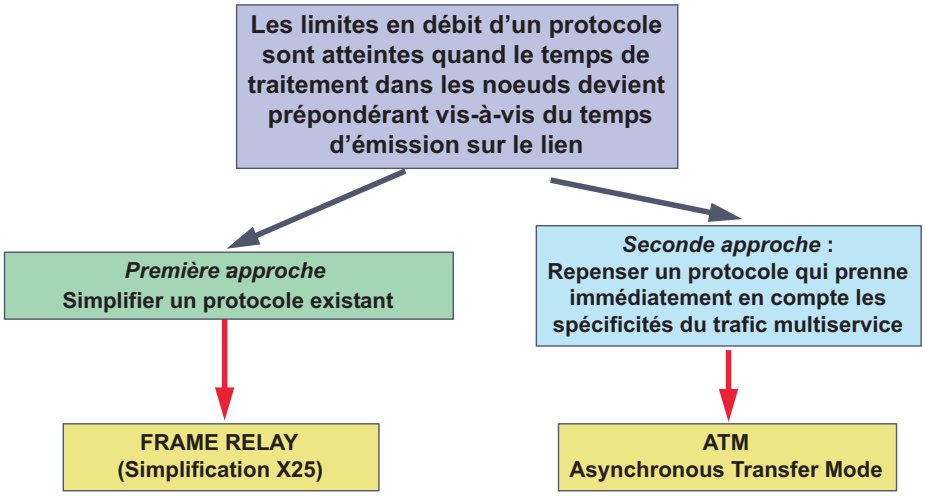

Les limites en débit d'un protocole sont atteintes quand le temps de traitement dans les noeuds devient prépondérant vis-à-vis du temps d'émission sur le lien
Première approche
Simplifier un protocole existant
Seconde approche :
Repenser un protocole qui prenne immédiatement en compte les spécificités du trafic multiservice
FRAME RELAY
(Simplification X25)
ATM
Asynchronous Transfer Mode

Figure 11.49 Différentes approches d'évolution des protocoles.

C'est dans le cadre de l'évolution du RNIS (**RNIS-LB**, RNIS Large Bande ou **B-ISDN**, *Broadband-ISDN*) qu'ont été développés le Frame Relay et l'ATM.

11.2.4 Le Frame Relay

D'X.25 au Frame Relay

La première approche d'allégement des tâches X.25 a concerné l'acheminement. Le champ adresse de la trame LAP-B étant inutilisé, il était possible d'y inscrire l'information d'indication du numéro de voie logique et de réaliser ainsi la commutation au niveau 2 (*Frame switching* ou commutation de trames). Ce principe est illustré figure 11.50.

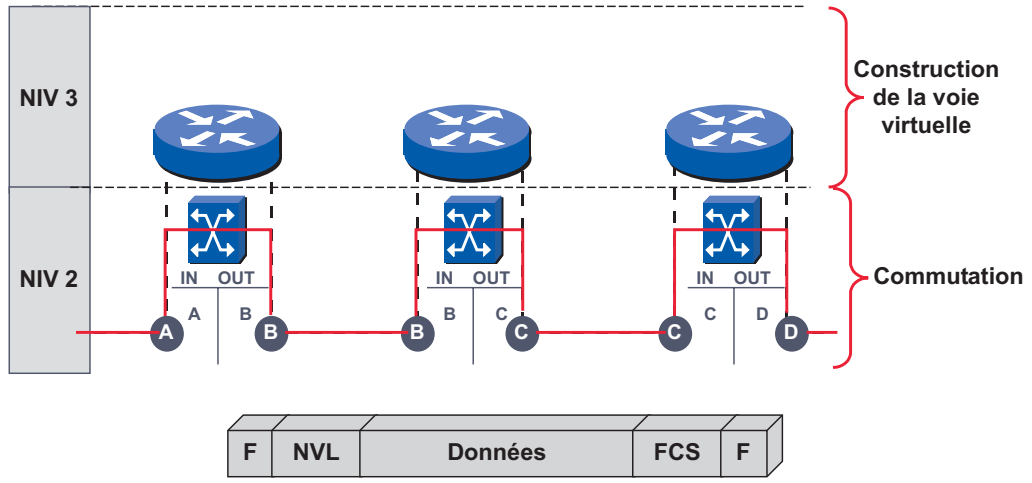


Figure 11.50 Première approche du Frame Relay.

Par la suite, toutes les fonctions, non liées directement à l'acheminement furent abandonnées pour donner naissance au **relais de trames** (*Frame Relay*) ou encore **LAP-F**. Initialement prévue pour une utilisation sur le RNIS (Canal D ou sur un ou plusieurs canaux B), la technologie Frame Relay a rapidement évolué, sous l'égide du Frame Relay Forum[8], vers un service de liaisons virtuelles permanentes, puis commutées utilisables sur tout support numérique hors RNIS.

Le relais de trames offre un service réseau en mode connecté conforme à l'avis Q.922 de l'UIT-T. La signalisation est du type canal sémaphore conforme à l'avis Q.933 (évolution de l'avis Q.931, protocole D du RNIS). Elle établit un service de liaison virtuelle entre les deux extrémités, qui peut être permanent (PVC, *Permanent Virtual Circuit*) ou établi à la demande (SVC, *Switched Virtual Circuit*). Actuellement, les opérateurs n'offrent qu'un service de circuits virtuels permanents.

Le relais de trames couvre les couches 1 et 2 du modèle OSI, mais n'est pas conforme à ce dernier. La couche physique émet un train de bits sur le support en assurant la transparence binaire (technique dite du *bit stuffing* ou de transparence binaire)

La couche 2 est subdivisée en deux sous-couches : le noyau (*Core*) et une sous-couche (**EOP**, *Element of Procedure*) complémentaire facultative. Non normalisée, ses fonctionnalités sont laissées à la discrétion de l'utilisateur. Cette sous-couche 2 supérieure peut, par exemple, être HDLC LAP-B. La répartition des fonctions essentielles est schématisée par la figure 11.51.

Format de l'unité de données

Le relais de trames utilise une trame de type HDLC (*High Level Data Link Control*) dérivée du LAP-D, délimitée par deux fanions (0x7E, 01111110B), elle comporte un champ adresse

8. Afin d'harmoniser les solutions, de combler les vides des normes et de proposer rapidement des solutions techniques cohérentes, les constructeurs se regroupent autour d'une technologie pour édicter leur propre règles : ce sont les forums constructeurs.

© Dunod – La photocopie non autorisée est un délit

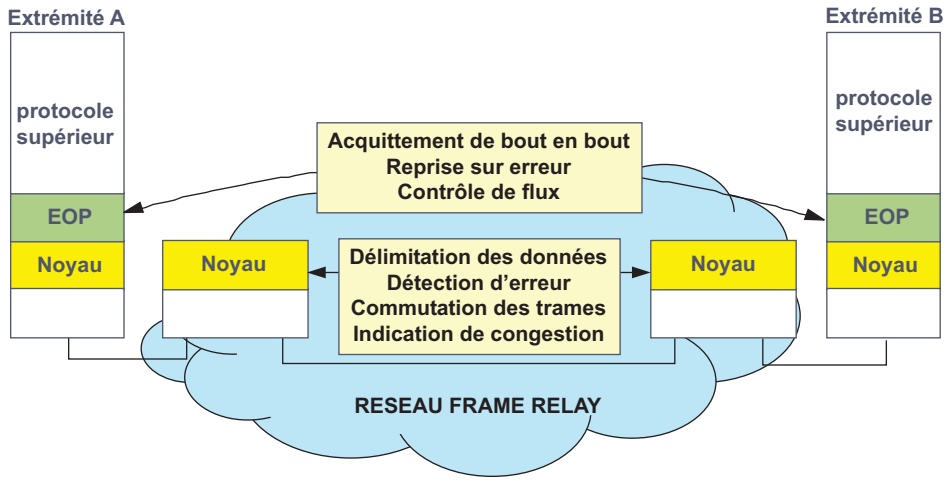


Figure 11.51 Architecture du relais de trames.

de 2 à 4 octets, un champ données et un champ de contrôle d'erreur (FCS). Le champ contrôle (commande) d'HDLC est absent, il est inutile puisqu'il n'existe qu'un seul type de trame (signalisation par canal sémaphore). La figure 11.52 représente la trame Frame Relay.

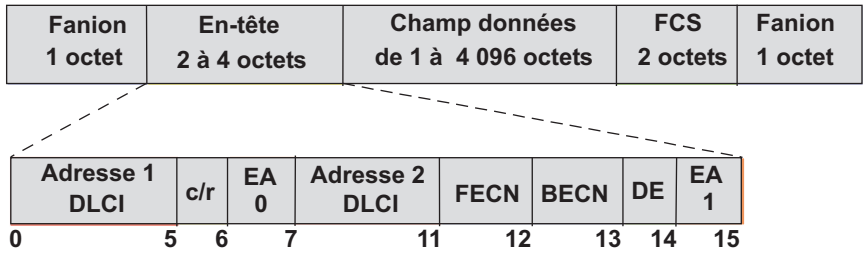


Figure 11.52 Trame Frame Relay.

Le champ adresse (**DLCI**, *Data Link Connection Identifier*) du relais de trames est subdivisé en plusieurs éléments. Dans la version de base, il est composé d'un premier bloc de 6 bits et d'un second de 4 bits (10 bits au total). Le champ **EA** (*End Address*) indique si le champ adresse a une suite (EA = 0) ou s'il est le dernier (EA = 1). Dans les versions étendues, le champ adresse est incrémenté de 1 octet (7 bits et le bit EA). L'adresse peut donc être exprimée sur 10 bits (version de base), 17 bits (en-tête de 3 octets) ou 24 bits (en-tête de 4 octets).

Le champ **C/R** (*Commande/Response*) a la même signification que le bit P/F (*Poll/Final*) d'HDLC. Les bits **FECN** (*Forward Explicit Congestion Notification*) et **BECN** (*Backward Explicit Congestion Notification*) sont utilisés pour signaler aux organes d'extrémité l'état de congestion d'un élément du réseau. Le bit **DE** (*Discard Eligibility*) est positionné par le réseau ou par les organes d'accès (**FRAD**, *Frame Relay Access Device*) il indique les trames à éliminer en priorité lors d'une congestion. Le FRAD est l'équipement interface entre le réseau de l'utilisateur et le réseau *Frame Relay*.

Mécanismes élémentaires

➤ Adressage dans le réseau

La connexion est établie à travers une liaison virtuelle, comparable à un circuit virtuel X.25, identifiée un identificateur de lien virtuel (**DLCI**, *Data Link Connection Identifier*) similaire au NVL d'X.25. Les DLCI 0 et 1023 sont réservés, le premier est réservé au protocole de signalisation (Q.933), le second pour la signalisation de la congestion. La connexion virtuelle (protocole orienté connexion) entre les extrémités résulte de la concaténation des DLCI (figure 11.53). À l'instar des NVL d'X.25, les DLCI n'ont qu'une signification locale. Dans la figure 11.53, la liaison virtuelle entre A et C résulte de la concaténation des voies logiques : 245, 18, 35 et 25.

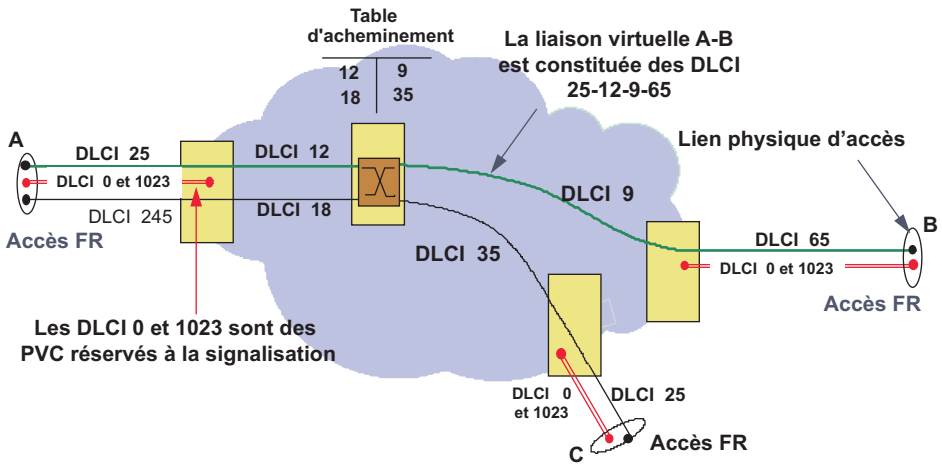


Figure 11.53 Acheminement dans le réseau.

Les tables d'acheminement sont établies sous la responsabilité de l'opérateur (PVC) ou du réseau lors d'une demande de connexion (SVC). Dans ce dernier cas, la demande d'établissement est acheminée par le protocole Q.933 (signalisation par canal sémaphore, DLCI 0).

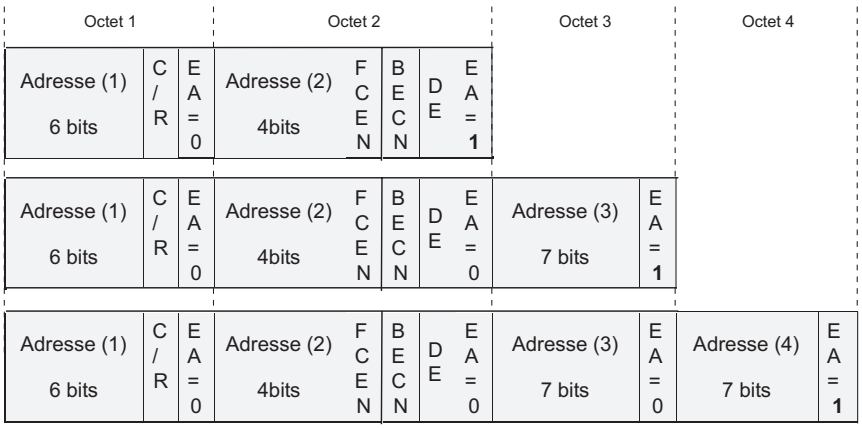


Figure 11.54 Format d'adressage étendu.

© Dunod – La photocopie non autorisée est un délit

Une capacité d'adressage sur 10 bits ne permet d'identifier que 1 024 (2^{10}) voies logiques, ce qui est suffisant pour la plupart des utilisateurs mais peut s'avérer faible pour l'identification des voies en interne dans le réseau. Aussi, un adressage étendu sur 17 et 24 bits est prévu (figure 11.54). Le format représenté correspond au format du Frame Relay Forum (les bits FCEM et BCEM ont une position fixe). Le tableau de la figure 11.55 décrit l'utilisation des diverses plages d'adressage pour l'adressage normal (10 bits).

DLCI	Utilisation
0	Établissement de circuits (Q.931)
1-15	Réservés
16-1007	DLCI utilisateurs (PVC, SVC)
1008-1018	Réservés
1019-1022	Multicast
1023	Signalisation de la congestion (CLLM ou LMI) et état des liens

Figure 11.55 Fonctions des différents DLCI à l'interface usager.

L'adressage des terminaux n'est pas fixé par la norme, le réseau peut spécifier des adresses de type E.164 (RNIS), X.121 (X.25) ou encore IP (TCP/IP).

➤ Le traitement des erreurs

Le traitement des erreurs n'est pas réalisé dans le réseau, chaque commutateur n'assure qu'une vérification d'intégrité de la trame :

– délimitation de la trame ;

– validation du DLCI ;

– contrôle d'erreur (FCS).

Toutes les trames non valides sont purement et simplement éliminées. Le traitement des erreurs est reporté sur les organes d'extrémité, il est confié aux protocoles de niveau supérieur, qui devront éventuellement mettre en œuvre des mécanismes de :

– numérotation des blocs de données pour la détection de perte ;

– reprise sur temporisation ;

– reprise sur erreur.

➤ Le contrôle d'admission

La simplification du protocole a conduit à la suppression de tout contrôle de flux dans le réseau et à fragiliser celui-ci face aux problèmes de congestion. Aussi, toute nouvelle connexion ne doit être acceptée que si le réseau est apte à la satisfaire sans préjudice pour les connexions déjà établies. Dans les réseaux de type X.25, le contrôle d'admission est effectué à l'établissement du circuit : dans chaque nœud sont réservées les ressources nécessaires au traitement des données (buffer), si il n'y a plus de ressources disponibles la connexion est refusée. Cependant, la réservation statique des ressources est incompatible avec l'admission d'un trafic en rafale qui rend le dimensionnement du réseau difficile. En Frame Relay, toute demande de connexion est accompagnée d'un descripteur de trafic définissant en particulier le débit moyen et le débit de pointe demandé. Un contrat de trafic est passé entre la source et le réseau ; il comporte trois paramètres :

– Le **CIR** (*Committed Information Rate*) ou débit moyen garanti. Le CIR caractérise le débit moyen contractuel que doit garantir le réseau. La connexion ne sera acceptée que si la somme des CIR sur le lien (ou sur le nœud) ne dépasse pas le débit maximal du lien (ou la capacité de traitement du nœud).
– **L'EIR** (*Excess Information Rate*) ou surdébit autorisé au-dessus duquel tout bloc de données soumis au réseau est détruit ;
– Le temps d'analyse du trafic (Tc).

Le CIR définit le volume moyen admis dans le réseau ou **Bc** (*Committed Burst Size*) tel que Bc = CIR · Tc. L'EIR précise le volume maximal autorisé tel que Bc + Be = (CIR + EIR) · Tc où **Be** (*Excess Burst size*) représente le volume excédentaire admis au-dessus du contrat Bc.

Si le volume du trafic soumis est inférieur à Bc tout le trafic soumis est transmis par le réseau. Si le volume de trafic soumis est compris dans l'intervalle]Bc... Be] les blocs de données sont transmis mais marqués (*Cell Tagging*). Lors de l'éventuelle traversée d'un nœud congestionné ces blocs seront éliminés. Les blocs transmis au-dessus de Be seront systématiquement éliminés. La figure 11.56 illustre ce propos.

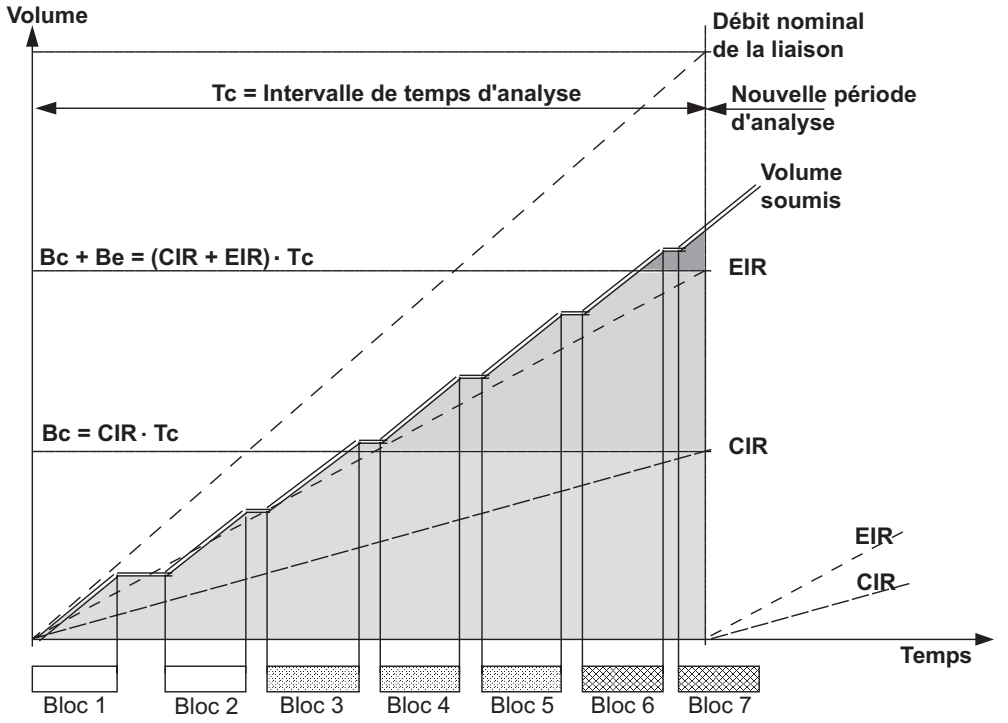


Figure 11.56 Contrôle de congestion dans les réseaux haut débit.

Les blocs 1 et 2 sont transmis normalement, à partir du bloc 3 le volume moyen garanti pour l'intervalle de temps T est dépassé, le bloc 3 et les suivants seront marqués comme dépassant le trafic moyen. Les blocs marqués (bit **DE**, *Discard Eligibility*) seront transmis, ils ne seront éliminés que s'ils traversent un nœud en état de congestion. Les blocs 6 et 7 excèdent le volume maximal autorisé, ils seront éliminés.

© Dunod – La photocopie non autorisée est un délit

L'élimination des blocs en excès n'est pas une solution satisfaisante. Il est préférable d'avertir les entités communicantes de l'état de congestion afin que, par autodiscipline, les sources ralentissent leur émission. Ce principe est illustré par la figure 11.57.

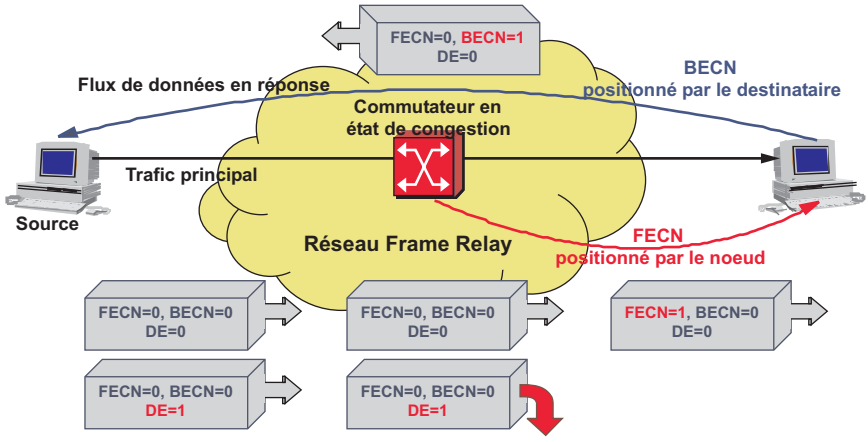


Figure 11.57 Notification de congestion.

Lorsqu'un bloc de données traverse un nœud en état de congestion, celui-ci positionne un bit pour avertir le destinataire d'un état de congestion en avant de la source (**FECN**, *Forward Explicit Congestion Notification*) et que des données ont pu être éliminées. Cette indication est transmise aux couches supérieures afin que celles-ci mettent en œuvre un mécanisme de contrôle de flux. Le destinataire profitera des données en réponse pour avertir la source que le circuit qui le dessert (circuit aval) est congestionné (**BECN**, *Backward Explicit Congestion Notification*).

Ce mécanisme n'est pas très efficace, car, l'équipement d'accès n'a pas toujours la faculté de réduire volontairement son flux d'émission. C'est notamment le cas d'un routeur interconnectant un réseau local. De plus, il suppose un trafic bidirectionnel ce qui peut introduire une inefficacité complète du système ou, du moins, une certaine inertie. Ce procédé est injuste. En effet, tous les hôtes dont les données transitent par le nœud congestionné sont invités à réduire leur trafic, même ceux qui ne sont pas responsables de cet état de fait. Pour y remédier un protocole spécifique a été développé : le **CLLM** ou *Consolited Link Layer Management*.

Les protocoles de gestion de la congestion

➤ Le protocole CLLM

Le protocole CLLM (origine ANSI T1 606) permet à tout nœud en état de congestion d'en avertir ses voisins et la source. Le message CLLM (*Consolided Link Layer Management*) contient la liste des voies logiques congestionnées et la cause de cette congestion. Le protocole CLLM est implémenté sur la trame **XID** de LAP-D (*eXchange IDentifier*).

➤ Le protocole LMI

Plus complet que le protocole **CLLM** (*Consolided Link Layer Management*), **LMI** (*Local Management Interface*) a été défini par le Frame Relay Forum pour prendre en charge toute la signalisation d'un réseau relais de trames. Le protocole LMI n'est disponible qu'à l'interface

usager (**UNI**, *User Network Interface*). Il utilise le DLCI 1023 (*Data Link Connection Identifier*), dernière voie logique identifiable dans l'adressage minimal à 10 bits, pour connaître l'état des circuits virtuels, de ce fait, les protocoles CLLM et LMI s'excluent mutuellement. Le protocole LMI (*Local Management Interface*) permet à l'utilisateur (**FRAD**, *Frame Relay Access Device*) de connaître à tout instant :

– L'état de ses circuits virtuels permanents (*Virtual Circuit Status*) par l'échange de messages questions (*Status Enquiry*, demande de statut) et de messages réponses (*Status*, état du lien).

– L'état du lien physique (*Link Status*) par échange de messages numérotés (*Keep Alive*).

– La modification du statut d'un lien (DLCI) sur l'initiative du réseau (messages asynchrones).

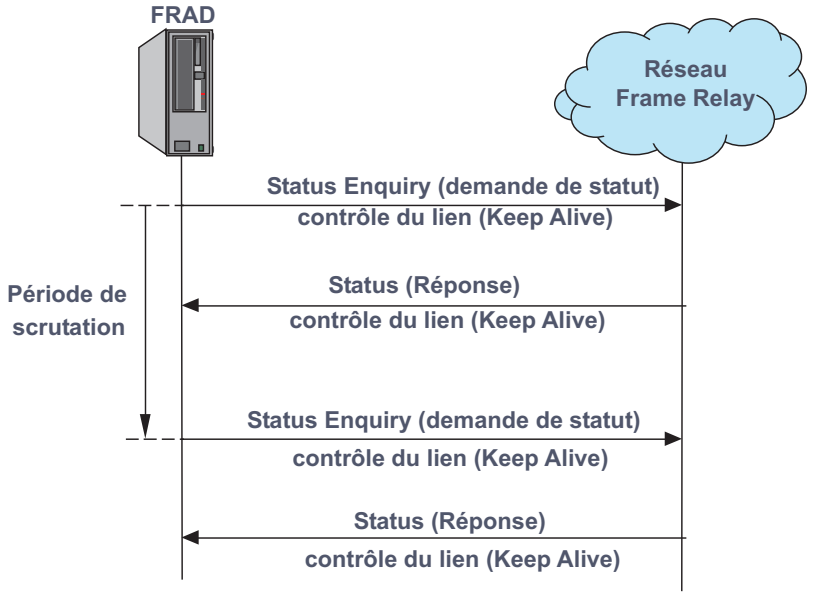


Figure 11.58 Échange de messages synchrones sur l'état des liens.

Les messages d'état du lien autorisent un contrôle de flux très efficace en signifiant à un équipement l'indisponibilité du lien (protocole de type XON/XOFF). La figure 11.58 symbolise l'échange de messages. La procédure de scrutation introduit un délai relativement important avant que le FRAD ne connaisse l'état d'un lien. La procédure asynchrone remédie à cet inconvénient, l'une des deux entités peut prendre l'initiative d'envoyer un message de demande de statut. Le protocole LMI utilise les trames non numérotées de LAP-D. Les messages comportent un en-tête fixe et une partie variable contenant les éléments d'information. Le champ discriminateur de protocole permet de distinguer le type d'architecture des couches supérieures. Le champ référence d'appel est toujours à 0, il n'est utilisé que dans le protocole Q.933 pour l'établissement des CVC. Le champ type de message identifie la commande. Les éléments d'information sont codés : type – longueur – information. La figure 11.59 représente deux exemples de message : une demande de statut pour un circuit virtuel permanent (CVP) et la réponse à cette demande.

© Dunod – La photocopie non autorisée est un délit

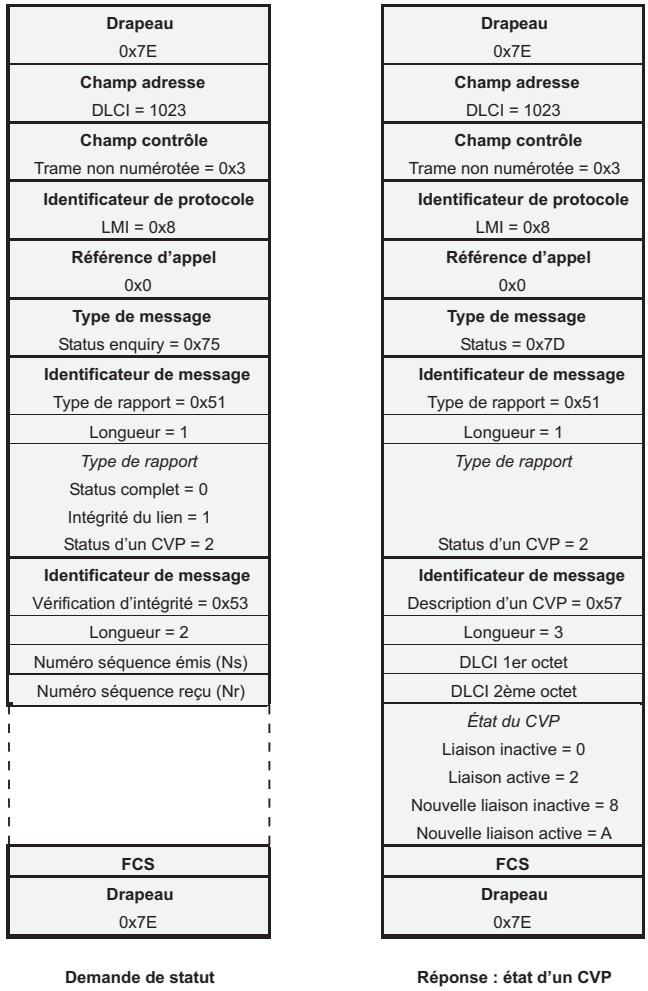


Figure 11.59 Exemple de messages LMI.

➤ Établissement de la connexion

Les circuits virtuels commutés (CVC ou SVC) sont établis à la demande de l'utilisateur[9]. Les CVC sont établis dans les deux sens (communication bidirectionnelle). Les messages d'établissement sont acheminés sur le DLCI 0 (Voie de signalisation bidirectionnelle).

Le message d'établissement est assez complexe. En effet, lors de la mise en service d'un CVP les différents paramètres de la liaison sont fixés à la souscription de l'abonnement et restent valables pendant toute sa durée. Ce n'est pas le cas des CVC. À chaque appel, les paramètres de la liaison demandée doivent être fournis (message *Setup*). La figure 11.60 illustre l'échange de messages lors de l'établissement d'une connexion et la libération du circuit virtuel.

9. L'établissement d'un circuit virtuel commuté est régi par la recommandation Q.933 dérivée de la recommandation Q.931.

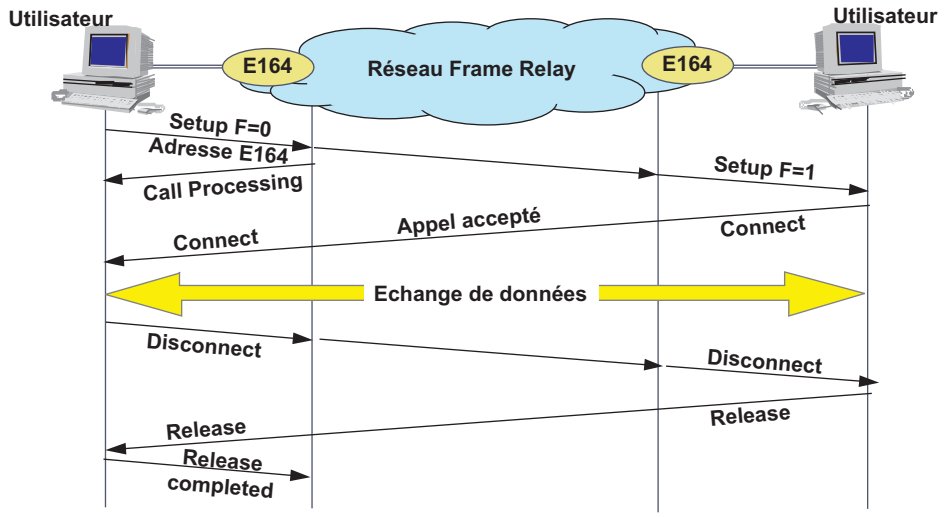


Figure 11.60 Établissement et libération d'une connexion commutée (SVC).

La demande de connexion (*Setup*) est acquittée deux fois, la première fois par le réseau (Signal de progression d'appel, *Call processing*) qui rend compte qu'il accepte la nouvelle connexion avec les paramètres précisés dans la demande et qu'il transmet celle-ci à l'appelé. Le message *Call processing* contient le DLCI affecté à la connexion (c'est le réseau qui détermine le DLCI à employer). L'appelé acquitte à son tour la demande de connexion (*Connect*). Le message est transporté en mode transparent par le réseau (celui-ci ne l'interprète pas). La figure 11.61 présente la structure du message de demande d'établissement.

La référence d'appel identifie tous les messages de supervision relatifs à une connexion. Elle n'a qu'une valeur locale (Usager/Réseau), chaque extrémité utilise une référence d'appel différente. Le bit F (*Flag*, drapeau) sert à discriminer un message appelant (F = 0) d'un message appelé (F = 1) ceci permet, lors d'une collision d'appel d'éviter, que la même référence d'appel ne soit utilisée.

Le champ relatant les capacités du réseau support (*Bearer Capability*) n'est présent que pour maintenir la compatibilité avec les évolutions futures, actuellement son contenu est fixe. Le numéro de DLCI est obligatoire dans le sens réseau/abonné (c'est le réseau qui fixe le numéro de DLCI). Facultatif dans le sens usager/réseau, le numéro de DLCI ne constitue qu'une proposition que le réseau accepte ou refuse. C'est le réseau qui, en dernier, détermine le numéro de DLCI à utiliser.

Les paramètres du noyau (élément d'information 0x90) fixe les paramètres utilisés dans chaque sens de la liaison (liaison bidirectionnelle, éventuellement dissymétrique), les paramètres fixés sont :

– La charge utile des trames (MTU, *Maximum Transfert Unit*).
– Le débit de la liaison (CIR).
– Le débit minimal acceptable (qualité de service).
– Le *Committed Burst Size* (Bc).
– *L'Excess Burst Size* (Be).

© Dunod – La photocopie non autorisée est un délit

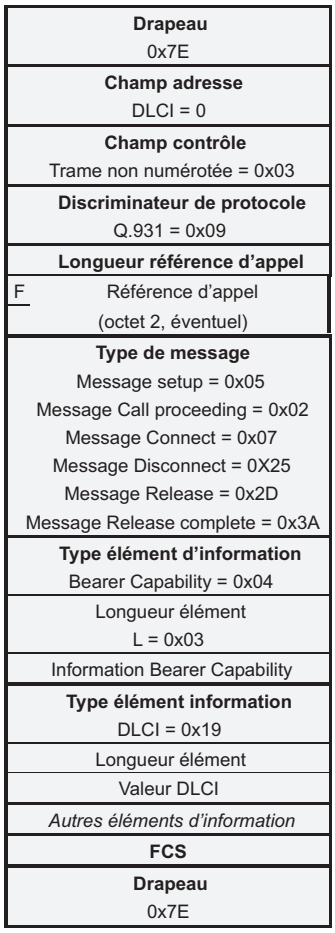


Figure 11.61 Structure du message d'établissement (message Setup).

Les adresses appelé/appelant (élément d'information : adresse appelé 0x70, adresse appelant 0x6C) sont décrites par les informations suivantes : le type d'adressage (RNIS : E.164, X.121 ou privé), la longueur d'adresse. L'adresse est codée en ASCII (IA5), 1 octet par caractère. Éventuellement, les paramètres de la sous-couche 2 supérieure peuvent être fixés : taille fenêtre et temporisateur.

Conclusion, le relais de trames et X.25

Indépendamment des progrès technologiques réalisés dans les commutateurs, le gain de performance obtenu avec le relais de trames résulte de la simplification du protocole et de la suppression de contrôles redondants. Le tableau de la figure 11.62 compare les tâches réalisées par chaque couche pour chacun des deux protocoles.

Le gain en vitesse de commutation du relais de trames par rapport à X.25 est de l'ordre de 5 à 10. Le succès actuel du relais de trames est essentiellement dû à sa simplicité face à ATM. Particulièrement adapté à l'interconnexion des systèmes exigeants en débit et générant

	X.25	Frame Relay
Niveau 1	Délimitation des trames Transparence binaire	Délimitation des trames Transparence binaire
Niveau 2	Type de trames Validité de la trame (contrôle d'erreurs) Contrôle de séquencement Gestion de la fenêtre Gestion des temporisations Acquittement éventuel	Validité de la trame (contrôle d'erreurs) Validité du DLCI (DLCI connu) Acheminement Éventuellement positionnement des bits ED, EFCN, BFCN.
Niveau 3	Type de paquets Contrôle de séquencement Gestion de la fenêtre Gestion des temporisations Acquittement éventuel Routage	

Figure 11.62 Comparaison des traitements X.25/Relais de trames.

des trafics sporadiques (réseaux locaux, applications client/serveur), il a été adapté au transport des flux isochrones comme la voix[10] (FRF11 et FRF12).

11.2.5 L'ATM (Asynchronous Transfer Mode)

Généralités

Le relais de trames n'est qu'une évolution d'HDLC (LAP-D). Peu adapté, en natif, au transfert des flux isochrones, il n'est parfois perçu que comme une solution temporaire au besoin de haut débit. Ses limitations sont essentiellement dues au traitement d'unités de données de taille variable. Pour pallier cet inconvénient, la recommandation FR11 (Frame Relay Forum 11) introduit, pour le traitement de la voix, la notion de trames de longueur fixe.

En traitant des unités de données de taille réduite et fixe (cellules), les temps de traitements sont considérablement réduits. On peut alors assurer leur commutation par des systèmes matériels (*hardware*) et non plus logiciels, ce qui autorise des débits de plusieurs centaines de Mbit/s.

C'est sur ces bases que le CNET (Centre Nationale Etude et de Télécommunication) a décrit, en 1982, une technique de multiplexage asynchrone (**ATD**, *Asynchronous Time Division*) qui allait donner naissance à l'ATM. L'ATM supporte des liaisons point à point, ou point à multipoint, il comporte trois couches dont les fonctions essentielles sont (figure 11.63) :

– assurer l'adaptation des cellules au système de transport physique utilisé (couche physique),
– effectuer la commutation et le multiplexage des cellules (couche ATM à proprement parler),
– adapter les unités de données (segmentation et réassemblage) des protocoles supérieurs à la couche ATM (couche **AAL***, ATM Adaptation Layer*) et mettre en place des mécanismes spécifiques à chaque type de données transportées.

10. Voir section 16.6.

© Dunod – La photocopie non autorisée est un délit

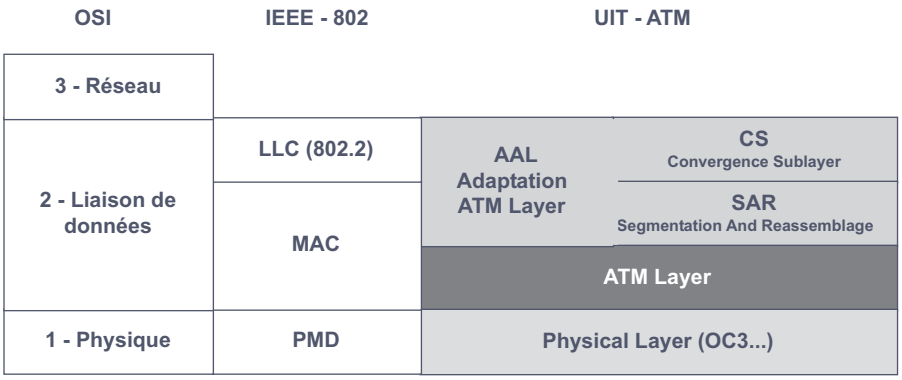


Figure 11.63 Architecture ATM.

L'ATM est une technologie en mode connecté, les données ne sont acheminées dans le réseau qu'après l'établissement d'une voie virtuelle (**VCC**, *Virtual Channel Connection*). Le circuit établi peut-être :

– bidirectionnel en mode point à point (unicast) ;

– unidirectionnel en mode point à multipoint (multicast).

Technologie orientée connexion, l'ATM peut, toutefois, émuler un mode de fonctionnement non connecté.

Taille des unités de données ou cellules

Étudié dans le cadre du développement du RNIS Large Bande (**B-ISDN**, *Broadband Integrated Service Digital Network*), l'ATM voit ses caractéristiques fortement conditionnées par le transfert de flux isochrone tel que la voix. Ce dernier point a été déterminant dans le choix de la taille des unités de données (cellules).

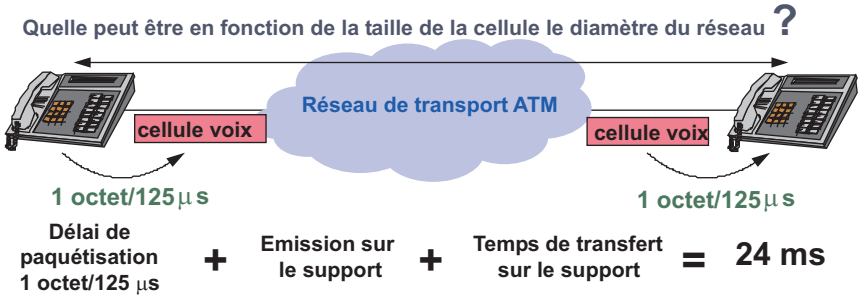


Figure 11.64 Temps de transfert d'une cellule voix.

En effet, un temps de transfert supérieur à 24 ms (temps fixé par l'UIT) implique l'utilisation, dans le réseau de transmission d'adaptateurs spécifiques, et la mise en service d'annuleurs d'écho. De ce fait, il s'agit de rechercher une taille de cellule compatible avec l'élongation envisagée du réseau (figure 11.64).

Compte tenu, d'une part que la paquetisation des données s'effectue à raison de 1 octet toutes les 125 μs (codage MIC) et, d'autre part en admettant une vitesse de propagation sur

le support de 2.10^8 m/s et un débit du lien de 64 kbit/s (voix MIC, G.711), le tableau de la figure 11.65 indique la distance maximale franchissable.

Taille de la cellule	Temps de paquetisation en ms	Temps de transfert sur le support	Temps de transport admissible en ms	Distance théorique en km
16	2	2	20	4 000
32	4	4	16	3 200
48	6	6	12	2 400
64	8	8	8	1 600
96	12	12	0	

Figure 11.65 Distance maximale franchissable sans annuleur d'écho.

Le tableau de la figure 11.65 montre que la limite maximale de la taille des unités de données est de 64 octets, c'est cette dernière taille qui avait été proposée à l'UIT par certains pays, notamment les États-Unis. En effet, compte tenu de la dimension de ce pays, le réseau de transport était déjà équipé de systèmes d'annulation d'écho, une taille de 64 octets présentait un meilleur rendement pour la transmission de données (rapport entre les données protocolaires et les données utiles). Pour des raisons inverses, les Européens préféraient une taille plus réduite : recherche de la distance maximale franchissable sans annuleur d'écho et meilleur rendement de multiplexage, ils proposèrent une taille de 32 octets. Finalement, un compromis a été adopté et la taille intermédiaire des unités de données (cellules) fut choisie, soit 48 octets.

Mécanismes de base et format de la cellule ATM

➤ L'adressage dans les réseaux ATM

À l'instar de X.25 ou du Frame Relay, l'ATM utilise en interne dans le réseau un adressage de convention identifiant les voies virtuelles (multiplexage par étiquette) et un adressage hiérarchique à la périphérie du réseau de type E.164 pour les réseaux publics (adressage du RNIS).

La taille des tables de commutation est l'un des facteurs principaux intervenant dans l'efficacité de la commutation. La commutation est d'autant plus rapide que la taille des tables de commutation est faible. Compte tenu de cette remarque, l'ATM, à des fins d'efficacité, utilise deux niveaux d'identification. En effet, dans un réseau plusieurs sources partent d'un même commutateur d'entrée et se dirigent dans une même direction (route). Plutôt que de gérer les N connexions, il est plus aisé de les regrouper (identifiant commun) et de ne traiter au cœur du réseau que cet identifiant de second niveau. Cette technique, qui permet un allégement des tables de commutation, est utilisée dans l'ATM (figure 11.66) :

– Le premier niveau identifie la voie virtuelle (**VCI***, Virtual Channel Identifier*). Il s'agit de l'identifiant d'une connexion semi-permanente ou établie à chaque appel.

– Le second niveau regroupe (agrégation de flux) un ensemble de voies virtuelles ayant une même destination (nœud intermédiaire ou interface d'usager) en un faisceau virtuel (**VPI**, *Virtual Path Identifier*). Le VPI est une connexion semi-permanente contrôlée par l'administrateur du réseau.

© Dunod – La photocopie non autorisée est un délit

Figure 11.66 La double identification d'ATM.

Les commutateurs de second niveau, appelés **brasseurs**, commutent l'ensemble des voies virtuelles affectées à un faisceau (acheminement selon le VPI), ce qui garantit des temps de commutation brefs. Les commutateurs sont généralement situés à la périphérie du réseau (commutateur d'accès), tandis que les brasseurs assurent la commutation des faisceaux virtuels en interne dans le réseau (figure 11.67).

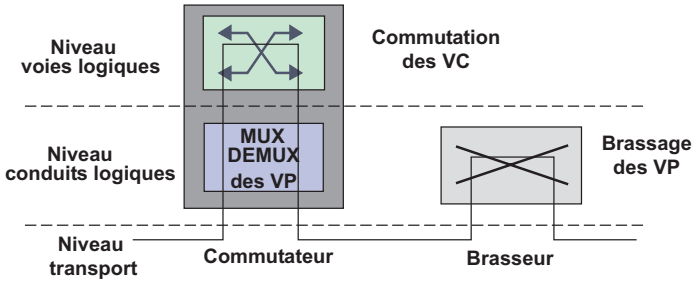


Figure 11.67 Le double niveau d'acheminement des cellules.

➤ Le contrôle d'erreur

Même si la fiabilisation des supports de transmission autorise un allégement du contrôle d'erreur, il reste cependant nécessaire de protéger le réseau contre l'acheminement erroné de blocs de données. À chaque commutateur, la validité des informations de routage (VPI/VCI) est contrôlée. Ne portant que sur l'en-tête de cellule, le champ HEC (**HEC**, *Header Error Control*) assure la détection d'erreur et la correction d'erreur simple (figure 11.68). Le champ HEC assure un contrôle d'erreur de type CRC sur l'en-tête, il autorise une autocorrection de l'en-tête pour les erreurs portant sur 1 bit (Distance de Hamming de 4). En cas d'erreurs non corrigées ou d'erreurs multiples, les cellules sont éliminées. L'octet de contrôle (dernier octet de l'en-tête) est le reste de la division booléenne (modulo 2) des quatre premiers octets de l'en-tête par le polynôme générateur : $G(x) = x^8 + x^2 + x + 1$, auquel est ajouté le polynôme $C(x) = x^6 + x^4 + x^2 + 1$ (addition booléenne soit un OU exclusif avec 01010101).

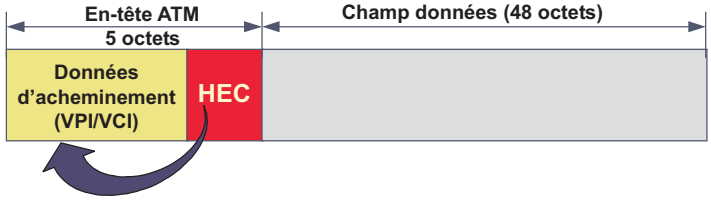


Figure 11.68 Portée du champ HEC.

Rappelons que la vérification de la validité des données utilisateurs est confiée aux couches supérieures des systèmes d'extrémité (*End Systems*).

➤ La délimitation des cellules

L'ATM n'utilise aucun fanion pour délimiter les cellules. Celles-ci ayant une taille fixe et une fréquence de récurrence élevée, il suffit de se positionner correctement sur un octet pour reconnaître les limites des cellules, c'est le champ HEC qui remplit cette fonction. Le HEC est calculé au fil de l'eau sur le flot de bits reçu dans un registre FIFO (figure 11.69). Lorsque le HEC est reconnu, le début de la cellule suivante (en-tête) se situe 48 octets plus loin. Un embrouillage du champ information élimine les risques de reproduction d'un « HEC » dans le champ données.

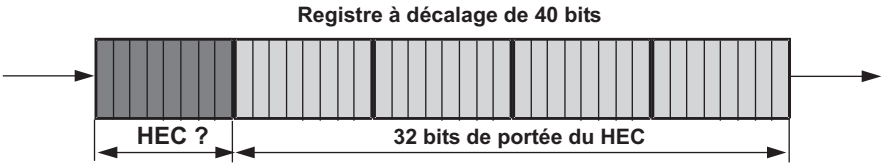


Figure 11.69 Principe du repérage du HEC.

➤ Formats de l'en-tête de cellule ATM

À des fins d'efficacité, l'en-tête ATM ne contient que les informations strictement nécessaires à l'acheminement, au contrôle du type de données et à la protection de l'en-tête. ATM utilise deux formats d'en-tête, selon que l'on se situe à l'interface usager/réseau (**UNI**, *User to Network Interface*) ou en interne dans le réseau (**NNI**, *Network to Network Interface*). La figure 11.70 représente ces deux formats.

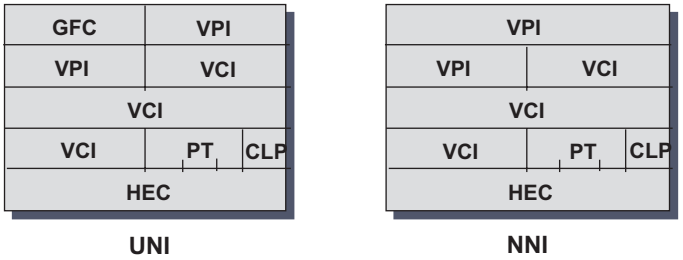


Figure 11.70 Formats de l'en-tête de cellule ATM.

Le champ **GFC** (*Generic Flow Control*) dont la normalisation n'est pas encore achevée devrait, en mode contrôlé (*Controled*), assurer le partage équitable de l'accès au réseau aux différentes stations dans une configuration point à multipoint. En mode point à point, le GFC devait permettre la résolution des conflits d'accès (résolution des contentions) et assurer le contrôle de flux à l'interface usager/réseau.

Sa présence est inutile dans le réseau, les quatre bits correspondants sont récupérés pour étendre le champ VPI des cellules NNI. Cette technique conduit à définir deux types d'en-tête de cellule. Selon que l'on se situe à l'interface usager/réseau (UNI) ou à une interface réseau/réseau (NNI) :

– Les cellules UNI identifient 65 536 VCI (16 bits) et 256 VPI (8 bits).
– Les cellules NNI identifient 65 536 VCI et 4 096 VPI (12 bits).

© Dunod – La photocopie non autorisée est un délit

Deux types de données transitent dans un réseau : les données d'origine utilisateur et les données internes au réseau (signalisation, maintenance...). Le champ **PT** (*Payload Type*) sur trois bits (bits 4, 3, 2 du quatrième octet) indique le type de charge contenue dans le champ données (figure 11.71).

Type Bit 4		EFCI Bit 3		User Bit 2	
0	Flux d'origine Usager (Cellules usager)	0	Bit EFCI (Explicit Forward Congestion Indication), pas de congestion	0,1	A disposition de l'application, peut être utilisé par la couche d'adaptation pour indiquer la
		1	La cellule a traversé au moins un nœud congestionné.		fin de la segmentation de l'unité de données (dernier fragment = 1)
1	Flux d'origine Réseau	0	Flux de maintenance	0	De section (Entre nœuds)
	(Cellules réseau)		(Cellules OAM)	1	De bout en bout
		1	Gestion des ressources	0	Réseau
			(Cellules RM)	1	Réservé

Figure 11.71 Signification du champ *Payload Type*.

Le traitement de la congestion est similaire à celui utilisé dans le relais de trames. Le bit de préférence à l'écartement (**CLP**, *Cell Loss Priority*) indique les cellules à éliminer en priorité lors d'un état de congestion. Le positionnement de ce bit est de la responsabilité de la source. Le bit CLP à 1 indique une cellule de priorité basse, à 0 il identifie une cellule de priorité haute.

Le bit CLP permet de spécifier, sur une même connexion, des flux différents. Il peut, par exemple, être positionné dans les transferts de vidéo compressée : les informations essentielles sont émises avec le bit CLP à zéro, les informations secondaires avec le bit CLP à un.

Les différentes couches du modèle

➤ Présentation

L'ATM comporte trois couches dont les fonctionnalités principales sont décrites ci-dessous. Les relations entre les différentes couches sont représentées en figure 11.72.

La couche **AAL** (*ATM Adaptation Layer*) garantit aux applications utilisateurs la qualité de service requise par l'application. Quatre types d'AAL sont proposés aux applications : AAL1, AAL2, AAL3/4 et AAL5. La couche AAL est divisée en deux sous-couches :

– La sous-couche de convergence (CS, *Convergence Sublayer*) destinée à incorporer les informations spécifiques au type d'AAL utilisé.

– La sous-couche de segmentation et de réassemblage (SAR, *Segmentation and Reassemblage*) adapte le format de l'unité de données issue de la sous-couche CS au format requis par ATM (cellules de 48 octets).

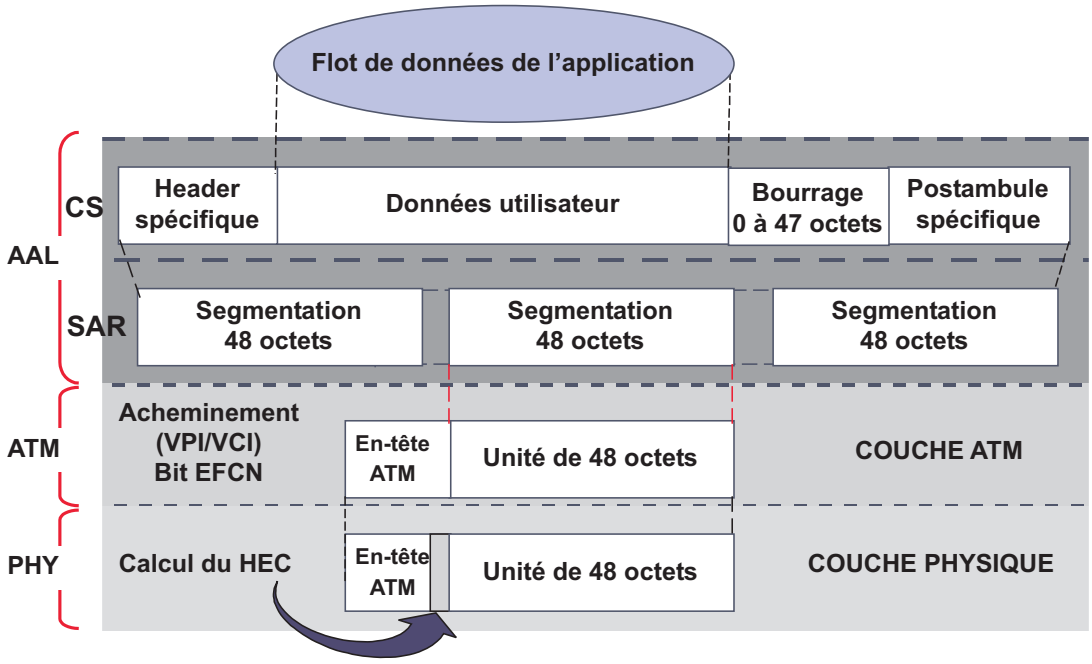


Figure 11.72 Relations entre les différentes couches de l'ATM.

La couche **ATM** est indépendante du sous-système de transport physique et des services d'applications qui l'utilisent. Elle assure les fonctions de multiplexage et démultiplexage des cellules, la génération et l'extraction des en-têtes, l'acheminement (commutation) des cellules et la translation des VPI/VCI enfin, le contrôle de flux (GFC, *Generic Flow Control*) à l'interface UNI (*User Network Interface*).

La couche physique (**PHY**) est chargée de fournir à la couche ATM un service de transport des cellules. Pour assurer, à la couche ATM, la transparence du support physique utilisé, la couche PHY est scindée en deux sous-couches :

– La sous-couche **TC** (*Transmission Convergence*) assure l'adaptation des débits, le contrôle des données (HEC) et la délimitation des cellules ;

– La sous-couche **PM** (*Physical Medium*) fournit l'accès au support physique et gère les mécanismes de synchronisation.

➤ La couche physique

Les modes de transmission

L'ATM est une technique de multiplexage asynchrone indépendante de l'infrastructure de transmission. Trois modes de fonctionnement ont été définis (figure 11.73) :

– Le mode **PDH** (*Plesiochronous Digital Hierarchy*) ou mode tramé temporel qui utilise les infrastructures de transmission existantes.

© Dunod – La photocopie non autorisée est un délit

– Le mode **SDH** (*Synchronous Digital Hierarchy*) ou mode tramé synchrone ou encore mode conteneur.
– Le mode cellules, mode dans lequel les cellules sont transmises directement sur le support de transmission. Le mode cellules est utilisé dans les infrastructures privées (liaisons spécialisées, privées ou louées) et les réseaux locaux.

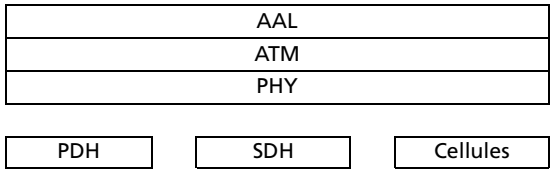


Figure 11.73 Les modes de transmission d'ATM.

L'adaptation des cellules ATM au réseau de transmission est réalisée par la sous-couche TC (*Transmission Convergence*). La sous-couche PM (*Physical Medium*) assure la transmission des bits sur le support.

La sous-couche TC

La sous-couche **TC** (*Transmission Convergence*) assure :

– l'adaptation des débits des sources au système de transmission ;
– le contrôle d'erreur ;
– la délimitation des cellules (synchronisation du système) ;
– l'adaptation des cellules au système de transmission.

Dans les systèmes de multiplexage par étiquette (ou statistique) il n'y a pas de relation directe entre le débit de la source et la capacité de transmission du système. Le maintien des horloges nécessite de réaliser un « bourrage » entre les unités de données. Cette fonction est assurée en HDLC par l'insertion de fanions. L'ATM n'utilise pas de fanions pour délimiter les cellules. Le bourrage est réalisé à partir de cellules vides[11] insérées pour combler « les silences ».

Chaque commutateur ATM réalise la fonction d'adaptation des débits par l'insertion et l'extraction de cellules vides. Les cellules vides sont identifiées par une valeur spécifique de l'entête : 0x00-00-00-01, seul le bit CLP, priorité à l'écartement, est positionné.

La sous-couche PM

La couche **PM** (*Physical Medium*) est chargée de la transmission et de la réception du flot de bits sur le support, elle réalise les fonctions suivantes :

– le codage ;
– l'alignement ;
– la synchronisation bit ;
– l'adaptation électrique ou opto-électrique au support.

11. Il faut entendre par cellule vide, une cellule ne contenant pas d'information.

➤ La couche ATM

La couche ATM est chargée :

– de l'acheminement des cellules dans le réseau ;

– de l'ajout et du retrait des en-têtes ATM ;

– du contrôle de flux (GFC, *Generic Flow Control*) à l'interface utilisateur (UNI) ;

– du contrôle d'admission en fonction de la qualité de service requise ;

– du lissage de trafic (*Traffic Shopping*).

La fonction d'acheminement

Rappelons que l'ATM introduit deux niveaux de commutation. L'un commute circuit virtuel par circuit virtuel, l'autre brasse un ensemble de circuits virtuels ayant une même destination et formant un même conduit virtuel.

La figure 11.74 illustre le mécanisme de la commutation. Le premier étage du commutateur effectue le multiplexage et démultiplexage des circuits virtuels, alors que le second étage les commute. Ainsi, la voie virtuelle 1 (VC1) du conduit virtuel 2 du port d'entrée 2 (VP2) est translatée en voie virtuelle 2 (VC2) et affectée au conduit virtuel 1 du port de sortie 3 (VP1).

Notons, qu'un commutateur achemine les cellules en fonction des données du couple VCI/VPI qui est modifié dans cette opération, alors qu'un brasseur n'utilise et ne modifie que le champ VPI.

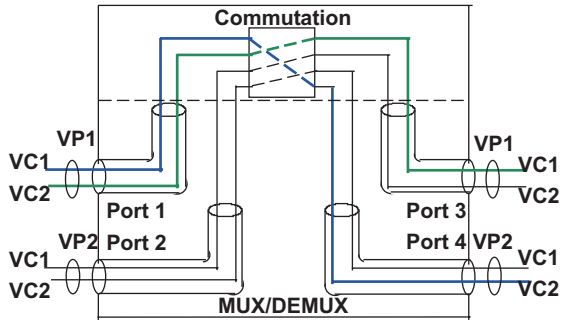


Table de commutation

Entrée		Sortie	
Port	VPI/VCI	Port	VPI/VCI
1	1,1	4	2,2
1	1,2	3	1,1
2	2,1	3	1,2
2	2,2	4	2,1

Figure 11.74 La commutation ATM.

Le contrôle d'admission (**CAC**, *Connection Admission Call*) a pour objectif de garantir une certaine qualité de service (**QoS**) à la connexion établie en termes de débit, perte de cellules et de variation de délai de transfert (gigue). À cet effet, l'ATM Forum a défini cinq classes de service[12] (**CoS**, *Class of Service*) pour garantir à l'utilisateur un service de transport en relation avec ses besoins.

12. À l'origine, l'IUT avait défini quatre classes de service, la classe A (débit constant, mode connecté), classe B (débit variable, mode connecté), classe C (débit variable, mode connecté) enfin classe D (débit variable mode non connecté), ces classes correspondaient directement aux AAL1, 2, 3 et 4. Proches l'une de l'autre, les AAL 3 et 4 ont été réunies en une seule, et remplacée par l'AAL5 par l'ATM Forum (simplification de l'AAL3/4). Dans le même temps l'ATM Forum redéfinissait les classes de services.

© Dunod – La photocopie non autorisée est un délit

Le contrôle d'admission n'est efficace que s'il existe un mécanisme permanent de surveillance qui s'assure que la source respecte les paramètres de trafic définis par le contrat de service. Cette surveillance est réalisée par une fonction spécifique **l'UPC** (*Usage Parameter Control*). L'UPC peut retarder une cellule, marquer une cellule à 1 (bit CLP, *Cell Loss Priority*), détruire une cellule et même demander la fermeture d'une connexion.

➤ La couche AAL

Applications et couche AAL

La technologie ATM est transparente aux données transportées (notion de mode de transport universel). De ce fait, il est nécessaire de réaliser, pour chaque type d'application, une adaptation spécifique afin d'affiner la qualité de service offerte aux applications, c'est le rôle de la couche **AAL** (*ATM Adaptation Layer*). Cinq types d'adaptations spécifiques ont été définis (figure 11.75).

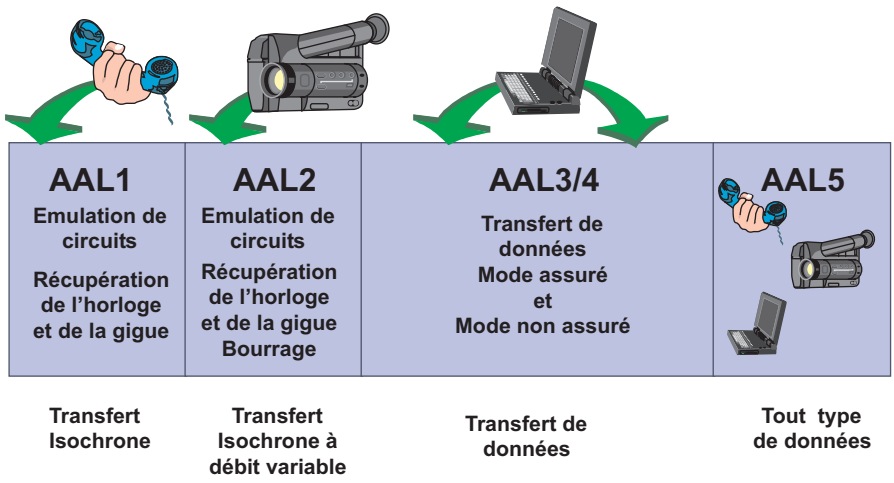


Figure 11.75 Les couches d'adaptation d'ATM.

La couche AAL1

La couche AAL1 permet un transfert isochrone par émulation de circuits, elle offre un service à débit constant (**CBR**, *Constant Bit Rate*). Elle n'assure que des fonctions minimales de segmentation et réassemblage, séquencement des unités de données et récupération de la gigue de cellules et de l'horloge. La figure 11.76 schématise le fonctionnement d'un système de récupération de gigue.

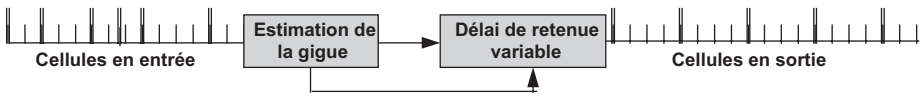


Figure 11.76 Principe de la récupération de gigue.

Les cellules sont mémorisées un temps équivalent au temps de transit maximal dans le réseau. La remise des cellules est alors asservie au flux moyen d'arrivée, ce qui, dans le cas de la voix et de la vidéo est suffisant. Cette technique est contraignante pour les transferts de voix

qui requièrent un temps de transfert de bout en bout inférieur à 24 ms, si le réseau n'est pas doté d'annuleur d'écho, et à 150 ms pour le confort de la conversation (effet satellite).

L'AAL1, conçue essentiellement pour les trafics de type isochrone non compressé, n'offre qu'un service CBR (*Constant Bit Rate*). Elle n'utilise pas les possibilités du multiplexage par étiquette et monopolise inutilement des ressources réseau (émulation de circuits).

La couche AAL2

La couche AAL2 diffère essentiellement de l'AAL1 par la possibilité de débit variable (**VBR**, *Variable Bit Rate*). L'AAL2, spécifique au transfert isochrone compressé (service VBR), assure la synchronisation des extrémités et offre une référence temporelle. Essentiellement destinée à la vidéo, l'AAL2 semble aujourd'hui abandonnée. En effet, la compression d'images de type MPEG-2 possède sa propre référence temporelle et, dans ces conditions, il semble plus efficace d'utiliser l'AAL5.

La couche AAL3/4

L'AAL3/4 regroupement des AAL3 et 4. Ces dernières avaient été étudiées pour les transferts de type données (flux sporadiques). Les AAL3 et AAL4 se différenciaient par l'approche mode connecté (AAL3) et non connecté (AAL4). Ces dernières ont été regroupées pour n'en former qu'une seule : l'AAL3/4. Celle-ci est aujourd'hui complètement abandonnée au profit de l'AAL5 plus efficace.

La couche AAL5

Proposée par l'ATM Forum, la couche AAL5 est une simplification de la couche AAL3/4 dont elle adopte la même architecture. Ces objectifs sont similaires mais elle offre un service plus efficace. La structure des données est représentée figure 11.77.

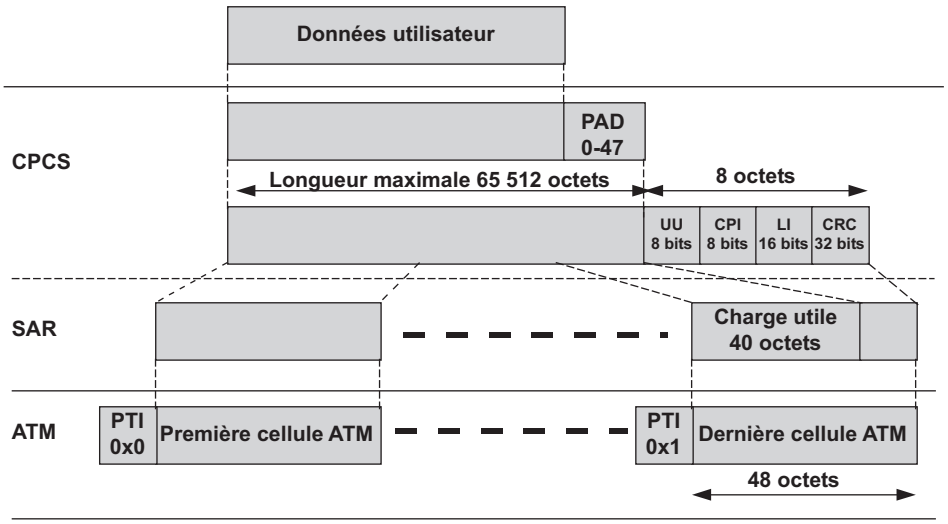


Figure 11.77 Structure de données de la couche AAL 5.

La couche AAL 5 autorise un transfert de données efficace, la SDU (*Service Data Unit*) est alignée sur un multiple de 48 octets (Champ **PAD**). Le champ **UU** (**CPCS UU**, *Service*

© Dunod – La photocopie non autorisée est un délit

Data Unit Common Part Convergence Sublayer User-to-User Indication) indique à l'usager le début, la suite et la fin du bloc de données. Le champ **CPI** (*Common Part Indication*) est utilisé pour aligner le suffixe (trailer) sur 8 octets, une utilisation future est en cours de définition. Le champ **LI** (*Length Indicator*) indique la longueur exacte des données utiles, tandis qu'un CRC sur 32 bits sécurise la SDU. Il n'y a pas de délimiteur de début et de fin, seul, le dernier bit du type de protocole (**PTI**, *Payload Type Identifier*) de l'en-tête ATM (bit 2 ou bit *Last Cell*) est à 1 dans le dernier fragment.

L'AAL5, définie par l'ATM Forum pour remplacer l'AAL3/4, semble la seule susceptible se subsister. Cependant, il serait nécessaire d'y apporter quelques modifications, notamment de pouvoir désactiver la détection d'erreur lors de transfert voix ou image peu sensible aux erreurs portant sur quelques bits. Des adaptations spécifiques (propriétaires) lui permettent d'assurer de manière efficace le transfert des flux voix (récupération des silences et de la gigue).

La qualité de service dans l'ATM

➤ Les classes de service de l'ATM Forum

L'un des principaux avantages d'ATM est de différencier les flux et de leur offrir une connexion en adéquation avec leur besoin : c'est la notion de **classe de service**. Les classes de service se répartissent en deux catégories, celles qui requièrent une qualité garantie comme les applications voix et vidéo et celles de la qualité « données » dont les exigences sont moindres. Les classes de service permettent à l'utilisateur de spécifier ses besoins : c'est la notion de **contrat de service**. Si le réseau a la capacité de satisfaire les demandes formulées, il accepte la connexion, sinon il peut proposer des paramètres de repli (figure 11.78).

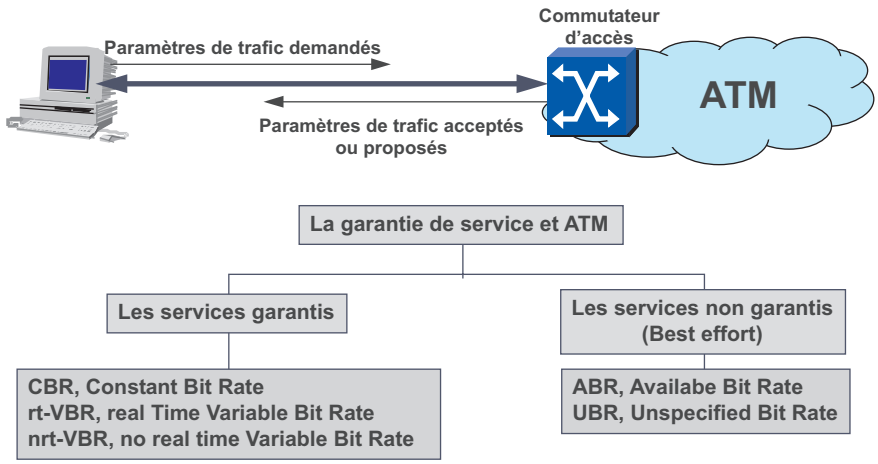

Commutateur d'accès
Paramètres de trafic demandés
Paramètres de trafic acceptés ou proposés
ATM
La garantie de service et ATM
Les services garantis
Les services non garantis (Best effort)
CBR, Constant Bit Rate
rt-VBR, real Time Variable Bit Rate
nrt-VBR, no real time Variable Bit Rate
ABR, Availabe Bit Rate
UBR, Unspecified Bit Rate

Figure 11.78 Contrat de service et classes de service.

La classe de service **CBR** (*Constant Bit Rate* ou **DBR**, *Deterministe Bit Rate*) définit un raccordement à débit constant qui correspond à une émulation de circuit. Elle est destinée aux applications de type voix ou vidéo non compressée. Le débit doit être garanti de bout en bout.

La classe **VBR** (*Variable Bit Rate* ou **SBR**, *Statistical Bit Rate*) s'applique aux trafics sporadiques, la connexion définit un débit minimal et un débit maximal. Pour les applications temps réel (*VBR-rt*, *VBR Real Time*) les variations maximales du délai de transfert sont déterminées

à la connexion. La classe VBR-rt correspond aux applications de type voix ou vidéo compressées. La classe VBR-nrt (*VBR no real time*) est généralement requise pour les applications de type transactionnel.

Les classes CBR et VBR garantissent aux applications une certaine qualité de service, le réseau doit s'adapter aux besoins de celles-ci. Cependant certaines, notamment les celles de type données, sont moins exigeantes en terme de débit. Afin de mieux utiliser les capacités du réseau, il semble préférable, dans ce cas, que ce soit les applications qui s'adaptent aux capacités de transfert de ce dernier et non l'inverse. La classe de service **ABR** (*Available Bit Rate*) ne spécifie, à la connexion, qu'un débit minimal et maximal, il n'y a aucun débit moyen garanti, les applications utilisent le débit disponible sur le réseau (entre les deux bornes prédéfinies). La classe ABR est adaptée à l'interconnexion de réseaux locaux.

De même, une classe de service de type datagramme ou *best effort* a été définie : **l'UBR** (*Unspeciefied Bit Rate*). L'UBR ne fournit aucune garantie de débit ni de remise des cellules. Si l'état du réseau le permet, toutes les cellules soumises sont transmises, en cas de congestion elles sont éliminées sans qu'aucun mécanisme d'avertissement de la source ni de demande de ralentissement de débit ne soit mis en œuvre. La classe UBR convient aux applications de type messagerie et sauvegarde à distance (*remote backup*).

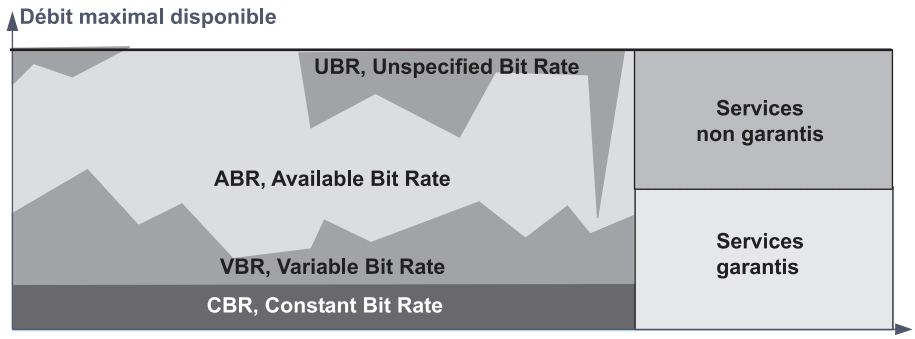


Figure 11.79 Partage de la bande passante selon la classe de service.

La figure 11.79 illustre comment la bande passante d'un conduit peut être partagée entre les différentes classes de service.

➤ Le contrat de service

Le contrat de service (*Connection Trafic Descriptor*) définit en termes de qualité de service (Qos) et de paramètres de trafic les caractéristiques de la connexion demandée. Trois variables définissent la qualité de service. Ce sont :

– **CTD** (*Cell Transfert Delay*) qui exprime le temps maximal garanti au transfert de bout en bout d'une cellule par le réseau.

– **CDV** (*Cell Delay Variation*) qui fixe la borne maximale des variations de temps de transfert des cellules (gigue), ce paramètre est très important pour les transferts de flux isochrone.

– **CLR** (*Cell Loss Ratio*) qui définit un taux de perte maximal des cellules transmises (CLR = nombre de cellules perdues/nombre de cellules transmises).

© Dunod – La photocopie non autorisée est un délit

Les paramètres de trafic sont :

– **PCR** (*Peak Cell Rate*) qui correspond au débit maximal qui sera soumis par la source et accepté par le réseau (débit de crête).

– **SCR** (*Sustainable Cell Rate*) qui précise le débit moyen envisagé soumis au réseau par cette connexion.

– **MBS** (*Maximum Burst Size*) qui définit la taille maximale des rafales admissibles par le réseau.

– **MCR** (*Minimum Cell Rate*) qui spécifie le débit minimum garanti par le réseau.

Le tableau de la figure 11.80 indique les paramètres valides en fonction de la classe de service invoquée

		Classes de service				
Paramètres		**CBR**	**VBR rt**	**VBR nrt**	**ABR**	**UBR**
Paramètres de QoS						
CTD	Cell Transfert Delay	•	•	•		
CDV	Cell Delay Variation	•	•			
CLR	Cell Loss Ratio	•	•	•	•	
Paramètres de trafic						
PCR	Peak Cell Rate	•	•	•	•	
SCR	Sustainable Cell Rate		•	•		
MBS	Maximum Burst Size		•	•		
MCR	Minimum Cell Rate				•	

Figure 11.80 Relation entre les paramètres du contrat de service et la classe de service.

Le contrôle de flux et de congestion

➤ Les mécanismes

Un réseau ATM est un réseau de files d'attente et comme tel, sensible à la congestion. Les mécanismes mis en œuvre pour la prévenir et y remédier sont similaires à ceux utilisés par le Frame Relay :

– élection de cellules à détruire en priorité en cas de congestion (bit **CLP**, *Cell Los Priority*). Le bit CLP peut être positionné à 1 par la source ou par tout commutateur si le flux, sur le circuit virtuel, dépasse le débit autorisé. CLP à 1 indique les cellules à écarter en priorité ; à 0, il identifie les cellules de priorité haute ;

– contrôle d'admission d'une nouvelle connexion dans le réseau (**CAC**, *Connection Admission Call*) consiste à n'accepter une nouvelle connexion que si celle-ci peut être satisfaite en terme de qualité de service requise sans préjudice de la qualité de service garantie aux connexions déjà actives ;

– contrôle du débit de la source (**UPC**, *User Parametre Control*) consiste à surveiller en permanence le débit de la source par rapport à un contrat de service défini à la connexion (SVC) ou à l'abonnement (PVC).

Le contrôle du débit de la source (UPC) définit trois niveaux :

– trafic est conforme au contrat de service, les cellules sont transmises ;
– trafic est supérieur au contrat de trafic, les cellules sont marquées. Le bit CLP est positionné par le commutateur (*Cell Tagging*). Les cellules marquées (CLP = 1) seront détruites si le flux traverse un commutateur en état de congestion ;
– trafic est supérieur au contrat de service et le réseau est en état de congestion, ou le trafic est très supérieur à ce dernier et les cellules sont alors éliminées (*Cell Discarding*).

➤ Le contrôle de congestion explicite

À l'instar du Frame Relay, l'ATM met en place un système d'information de l'état de congestion (**EFCN**, *Explicit Forward Congestion Notification*). Le mécanisme est similaire, lorsqu'un commutateur est en état de congestion (seuil de remplissage des buffers), il positionne le bit **EFCI** (*Explicit Forward Congestion Indication*) du champ **PTI** (*Payload Type Identification*). Le destinataire du flux est alors informé que les cellules ont traversé un commutateur congestionné (figure 11.81).

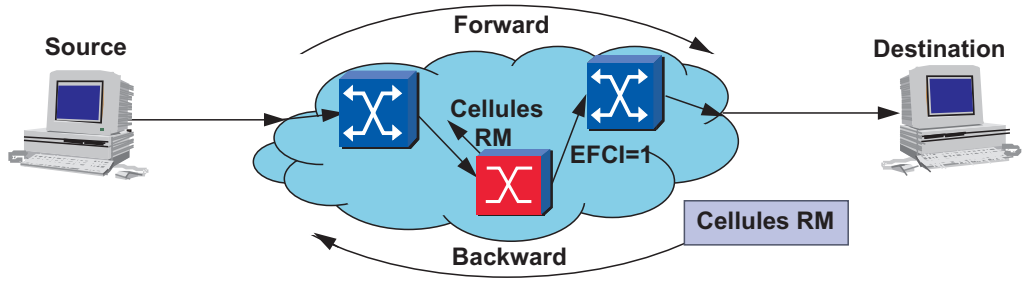


Figure 11.81 Mécanisme de signalisation de la congestion.

Le destinataire envoie alors à la source des cellules spécifiques pour l'informer de cet état et lui demander de réduire son débit (cellules **RM**, *Ressource Management*), cette méthode est dite : **BECN** (*Backward Explicit Congestion Notification*). Les commutateurs en état de congestion peuvent de même, insérer des cellules RM dans les flux en direction de leurs usagers pour leur demander de réduire leur débit (cellules RM dites **RR**, *Relative Rate*) ou les informer explicitement du débit disponible (cellule RM dites **ECR**, *Explicit Cell Rate*) en termes de débit maximal autorisé et du débit minimal garanti. Les cellules RM utilisent le VCI 6, le champ PT de la cellule ATM étant positionné à 110.

La signalisation et le routage

➤ Généralités

La signalisation est un ensemble de procédures destinées à l'établissement dynamique, au maintien et à la fermeture d'une connexion virtuelle commutée (non permanente). Compte tenu des éléments à prendre en compte, notamment la qualité de service (QoS), la signalisation ATM est relativement complexe. De type **CCS** (*Common Channel Signaling*) ou signalisation par canal sémaphore, elle diffère selon que l'on se situe à l'interface usager d'un réseau public ou privé, à l'interface entre deux réseaux privés ou publics (figure 11.82).

© Dunod – La photocopie non autorisée est un délit

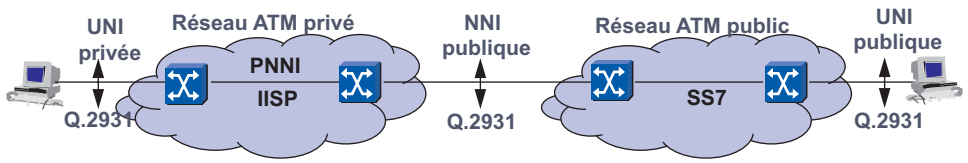


Figure 11.82 La signalisation dans ATM.

À l'interface usager (**UNI**, *User Network Interface*) ou entre réseaux (**NNI**, *Network to Network Interface*) une signalisation de type canal sémaphore (PVC 0/5) utilise le protocole Q.2931. Les réseaux publics utilisent la signalisation définie pour le RNIS, SS7 (*Signaling System 7*) ou CCIT N°7. En interne, les réseaux privés utilisent **PNNI** (*Private Network to Network Interface*) qui autorise l'établissement de SVC et assure un routage en fonction de la qualité de service. Précédemment **IISP** (*Interim Inter Switch Protocol*) ne permettait qu'une configuration statique du réseau, ce qui le réservait aux petits réseaux

➤ Architecture générale de la signalisation

La signalisation à l'interface usager (UNI) dérive des spécifications Q.2931, protocole de niveau 3, elle s'appuie sur une AAL sécurisée définie à cette intention : la **SALL** (*Signaling AAL*, Q.2100). De type canal sémaphore, la signalisation utilise le couple VPI/VCI réservé : 0/5 (VPI = 0, VCI = 5). La figure 11.83 représente l'architecture de signalisation telle que l'a définie l'ATM Forum.

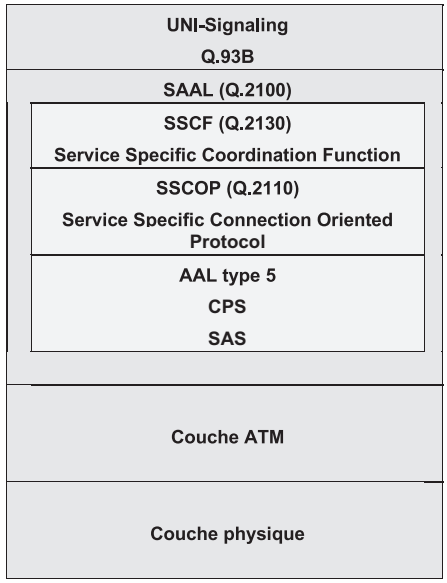


Figure 11.83 L'architecture générale de la signalisation NNI.

En mode commuté, l'établissement d'un SVC est préalable à l'envoi de données. Le message *Setup* est émis par l'appelant, il comporte tous les éléments nécessaires à l'établissement d'un SVC (bidirectionnel). Compte tenu de sa taille, ce message est composé de plusieurs cellules ATM émises sur le VPI/VCI réservé : 0/5.

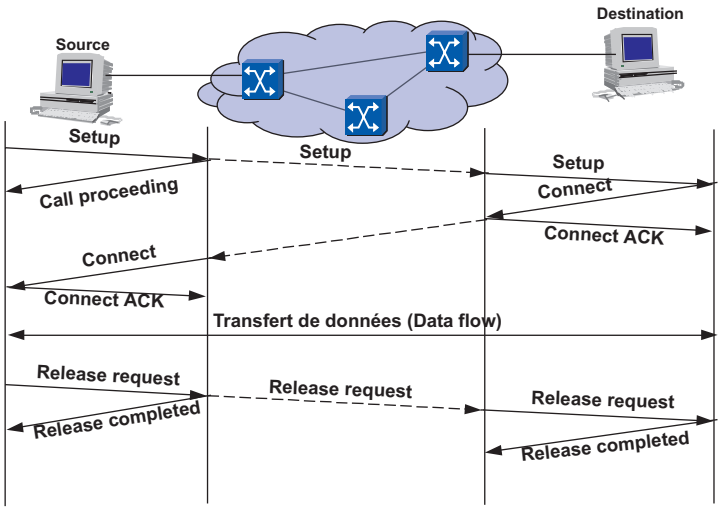


Figure 11.84 Diagramme des messages d'établissement.

Le message *Setup* est acheminé par le réseau qui détermine le meilleur chemin en fonction de la QoS requise. Le message *Call Proceeding* indique à l'émetteur que sa demande a bien été prise en compte, qu'elle est acceptée par le commutateur d'accès et que celui-ci transmet sa requête. Si la connexion est acceptée de bout en bout, le message est acquitté par le message *Connect* qui fixe le couple VPI/VCI à utiliser. La figure 11.84 présente le diagramme d'échange de messages lors de l'établissement et de la rupture d'un SVC.

Le message *Setup* contient toutes les informations nécessaires à l'établissement du SVC :

– Adresse source et destination.
– La bande passante demandée (**UCR**, *User Cell Rate*).
– La QoS par indication de la classe de service (CBR, VBR, ABR, UBR).
– Le type d'AAL requis.

➤ Le routage PNNI

PNNI (*Private Network to Network Interface*) est un protocole de routage du type état des liens (*link status*). Pour établir un SVC répondant à la QoS exigée, chaque commutateur doit avoir connaissance de la topologie du réseau et des caractéristiques de trafic disponibles sur les différents commutateurs du réseau :

– Débit disponible (*Available Cell Rate*).
– Délai de transfert (*Maximum Cell Transfer Delay*).
– Variation du délai de transfert ou gigue (*Cell Delay Variation*).
– Taux de perte de cellules (*Cell Loss Ratio*).
– Débit maximal admissible (*Maximum Cell Rate*).

Pour éviter un échange d'information prohibitif, PNNI segmente le réseau en groupes de commutateurs hiérarchisés (*peer group*). Un *peer group* est constitué d'un ensemble de nœuds

© Dunod – La photocopie non autorisée est un délit

logiques (les nœuds physiques sont les nœuds réels au plus bas de la hiérarchie). Dans chaque groupe, un commutateur maître est désigné. Chaque commutateur informe le maître de son état et récupère auprès de celui-ci les informations sur l'état des autres membres du groupe, de ce fait tous les membres du groupe ont une vision identique du groupe. Chaque commutateur maître du niveau N appartient au *peer group* du niveau $N + 1$, cette double appartenance permet au maître de renseigner ses homologues de la topologie du groupe subordonné. De même, chaque commutateur du niveau N est informé de la topologie des autres groupes par son maître. Chaque commutateur dispose alors d'une cartographie simplifiée du réseau à partir de laquelle il va effectuer un routage à « tâtons ». La figure 11.85 schématise cette architecture.

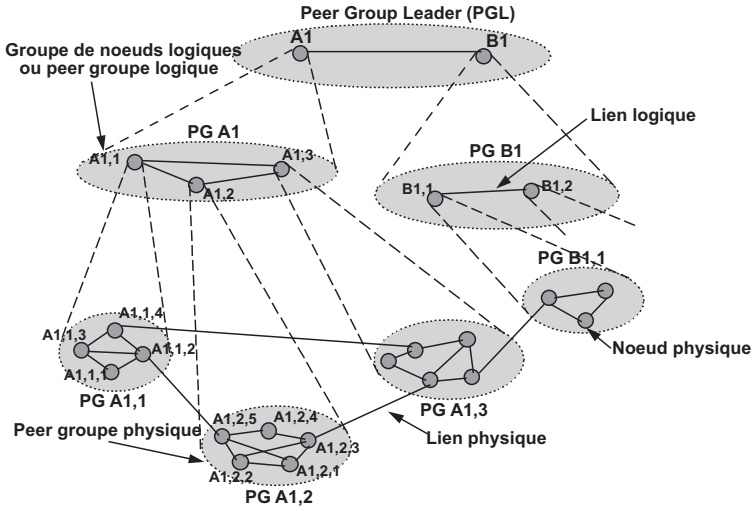


Figure 11.85 Architecture logique du réseau selon PNNI.

En fonction de la qualité de service requise par la demande d'établissement, le commutateur d'accès effectue un contrôle d'admission (**CAC**, *Connection and Admission Control*). Si le commutateur d'entrée peut accepter la connexion, à partir de sa connaissance de l'état du réseau, il établit une liste spécifique de routage (**DTL**, *Designated Transit List*) contenant les commutateurs répondant aux exigences de la demande. Le commutateur transmet alors la demande au commutateur suivant en y annexant la liste de routage (routage similaire à un routage par la source).

Chaque commutateur de la liste effectue un contrôle d'admission, s'il accepte la demande il la transmet au suivant dans la liste de routage. S'il ne peut accepter celle-ci (son état est différent de l'état connu par le commutateur source), il réachemine la demande vers le commutateur précédent qui recalcule une route (*Grank Back Fonction*).

➤ L'adressage dans les réseaux ATM

La fonction essentielle d'un processus de routage est de mettre en relation deux entités adressées. Ce qui nécessite, en principe qu'elles appartiennent au même espace d'adressage. Ce n'est pas toujours le cas pour les réseaux ATM. L'adressage dans les réseaux publics utilise le format E.164 de l'UIT (15 chiffres), tandis que l'adressage dans les réseaux privés supporte deux types d'adressage différents : les adresses NSAP (ISO) et une extension de l'adressage E.164.

Les adresses privées ATM, définies par l'ATM Forum, comportent deux parties, l'une identifie le réseau de raccordement (*network prefix* ou préfixe réseau) c'est-à-dire l'adresse WAN, l'autre à la disposition de l'utilisateur identifie le système d'extrémité (**ESI**, *End System Identifier*) et l'application utilisateur (**SEL**, *SELector field*).

La figure 11.86 représente le format général des adresses privées utilisées dans ATM. Le champ **AFI** (*Autority Format Identifier*), sur 1 octet, indique l'autorité de gestion et le format utilisé pour représenter l'adresse.

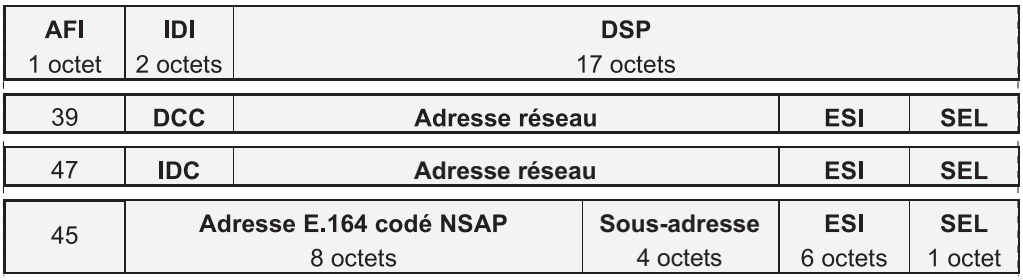


Figure 11.86 Structure des adresses privées ATM.

Les adresses **DCC** (*Data Country Code*) et **IDC** (*International Designator Code*) sont réservées à l'adressage des réseaux ATM des opérateurs privés, tandis que les adresses au format E.164 concernent l'adressage des réseaux privés et peuvent être vus comme une extension, chez la personne privée de l'adressage du réseau public (sous-adresse privée).

Le champ **IDI** (*Initial Domain Identification*), sur 2 octets, spécifie le domaine d'adressage. Enfin, le champ **DSP** (*Domain Specific Part*) correspond à l'adresse effective du terminal.

L'administration des réseaux ATM

L'ATM Forum n'a pas retenu, pour l'administration des réseaux ATM, les principes énoncés par l'ISO. Il a défini un protocole **ILMI** (*Interim Local Management Interface*) s'appuyant sur le protocole **SNMP** (*Simple Network Management Protocol*).

Le protocole **ILMI** (*Interim Local Management Interface*) introduit par la RFC 1695 fournit les informations de statut, de configuration et de diagnostic du système, il est aussi utilisé pour l'enregistrement d'adresse (extension du protocole).

Basé sur les agents SNMP et l'AAL5, ILMI utilise les commandes SNMP sur un VCC (*Virtual Circuit Connection*) réservé (VPI = 0, VCI = 16 noté 0/16). La figure 11.87 illustre l'architecture du système d'administration.

Une extension de la MIB[13] (*Management Information Base*) ILMI, la MIB ATM autorise l'accès aux informations des commutateurs ATM.

© Dunod – La photocopie non autorisée est un délit

13. Une MIB est un ensemble d'information d'admistration réseau.

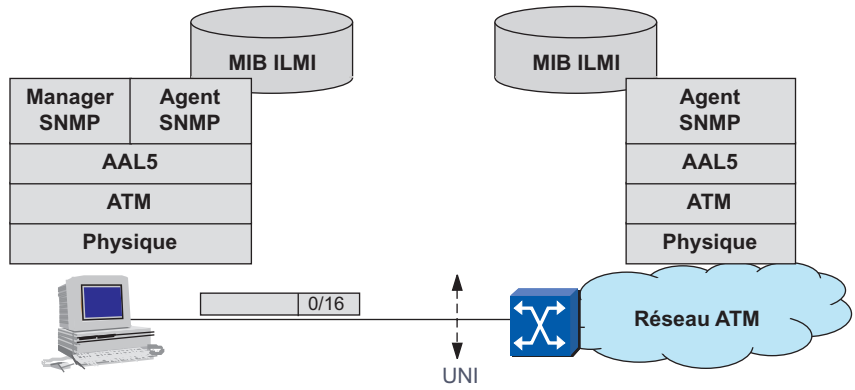


Figure 11.87 L'administration des réseaux ATM.

Conclusion

Autorisant un partage optimal de la bande passante, l'ATM est aujourd'hui le protocole de cœur de réseau utilisé par la majorité des opérateurs. Outre l'aspect performance, l'ATM permet de garantir aux utilisateurs une certaine qualité de service de bout en bout.

Compte tenu de la complexité d'établissement d'une liaison virtuelle qui tienne compte des paramètres de qualité de service, les opérateurs n'offrent qu'un service de connexion permanente. L'ATM n'est pas un protocole de bout en bout comme l'est TCP/IP, ce n'est qu'un protocole de transport. Les données utilisateurs doivent donc être encapsulés, ceci conduit à des empilements protocolaires fortement pénalisant. Des travaux en cours (figure 11.88) tendraient à appuyer les protocoles utilisateurs (TCP/IP) sur la couche transmission (SDH) voire directement sur la couche optique.

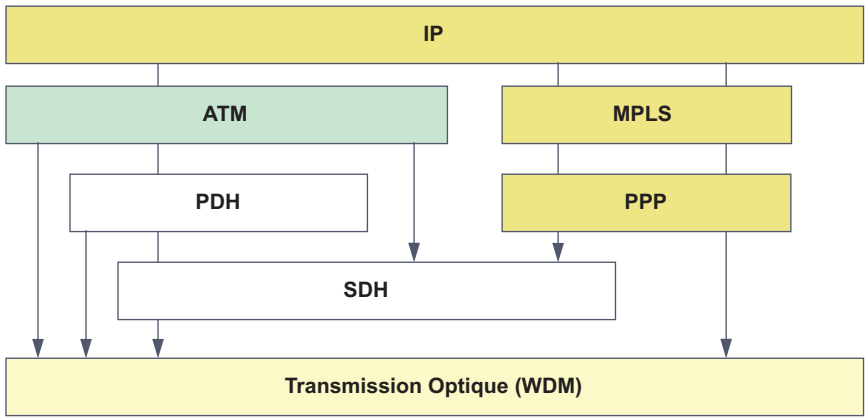


Figure 11.88 Évolution de l'architecture protocolaire des réseaux.

L'utilisation simultanée de MPLS et de PPP permet le transport des flux IP sur SDH, voire directement sur un canal optique (**WDM**, *Wavelength Division Multiplexing* ou multiplexage de longueur d'onde).

11.2.6 Les réseaux d'opérateurs

Généralités

Les réseaux d'opérateurs assurent deux fonctions essentielles, la collecte des flux des différentes sources par un ensemble de liens formant le réseau d'accès, et l'acheminement de ce trafic par leurs réseaux dits de transit. Certains opérateurs n'assurent que l'une des deux fonctions, on distingue alors les opérateurs de boucle locale et les opérateurs de transit. On appelle point de présence (**PoP**, *Point of Presence*) l'interface d'interconnexion entre le réseau d'accès et le réseau de transit (figure 11.89).

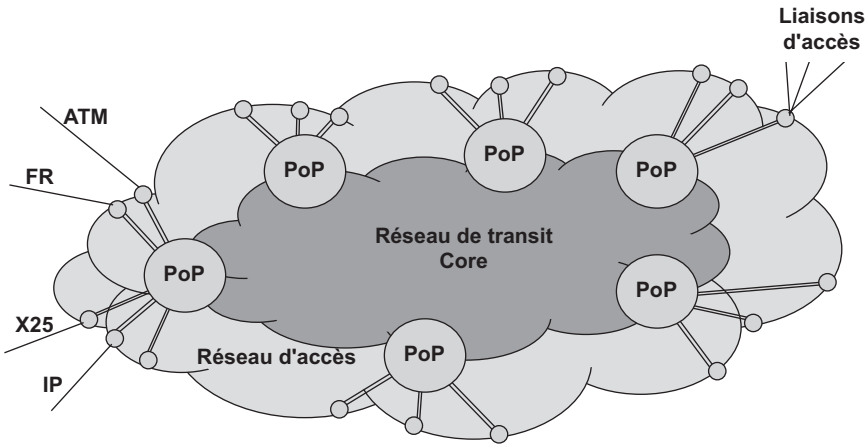


Figure 11.89 Architecture du plan de service.

Les réseaux IP

La plupart des réseaux d'opérateurs mettent en œuvre le protocole ATM, alors que la majorité des utilisateurs utilisent le protocole TCP/IP. On désigne sous le nom de réseau IP, l'infrastructure de l'opérateur destinée à acheminer le trafic IP. Le trafic IP peut être tout simplement encapsulé dans l'ATM via l'AAL5 (figure 11.90). Dans ce cas, il ne peut être tenu compte de la qualité de service, seul l'UBR est alors possible.

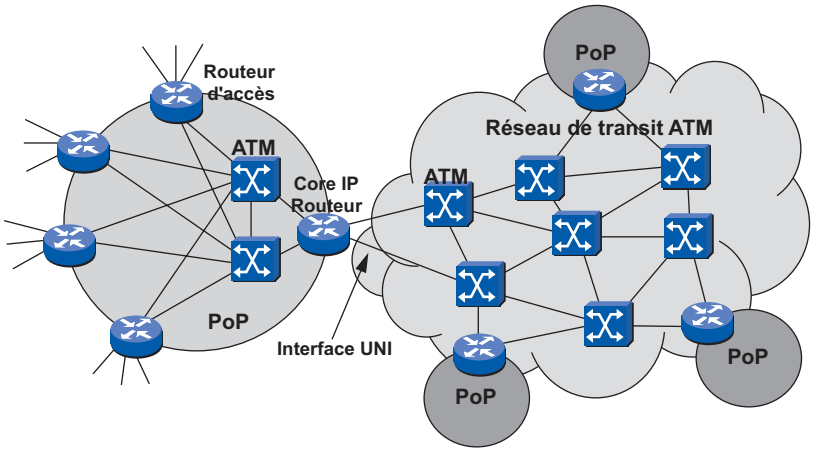


Figure 11.90 Réseaux IP/ATM.

© Dunod – La photocopie non autorisée est un délit

Cependant l'utilisation du protocole MPLS[14] (*MultiProtocol Label Switching*) peut permettre d'assurer un trafic différencié (DiffServ) par distribution des labels et mappage de ceux-ci sur une voie ATM (figure 11.91).

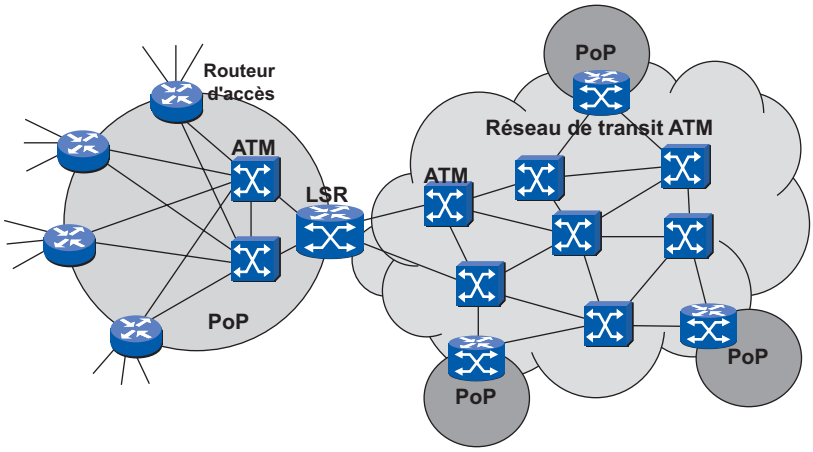


Figure 11.91 Réseaux IP/MPLS.

Les routeurs d'interface (*Core IP Router*) sont remplacés par des commutateurs/routeurs qui attribuent un label MPLS aux datagrammes IP (**LSR**, *Label Switching Router*). Remarquons que chaque routeur d'accès et LSR dispose, pour des raisons de sécurité, d'un double attachement aux commutateurs ATM.

11.3 L'ACCÈS AUX RÉSEAUX, LA BOUCLE LOCALE

11.3.1 Définition

La boucle locale correspond à l'ensemble des moyens mis en œuvre par un opérateur pour collecter le trafic des utilisateurs. Une définition plus restrictive limite l'utilisation du terme boucle locale au seul câble de raccordement usager/réseau. Pour des raisons historiques, l'infrastructure du réseau de boucle locale correspond à celle de la distribution des services voix. Cette infrastructure est aujourd'hui partagée entre les accès aux réseaux voix et les accès aux réseaux de données.

11.3.2 Organisation de la distribution des accès

Les moyens d'accès se répartissent en deux catégories, les accès aux réseaux d'opérateurs (opérateurs de boucle locale) et les moyens fournis à l'usager pour raccorder ses propres sites informatiques et réaliser ainsi un réseau privé (opérateur de liaisons louées). La figure 11.92 illustre cette approche.

La réalisation d'un réseau de distribution (collecte) nécessite des investissements importants. Dans la plupart des pays, ces réseaux ont été financés par des ressources publiques. La mise en concurrence des télécommunications a donc posé le problème du partage de cette

14. Voir section 8.5.2.

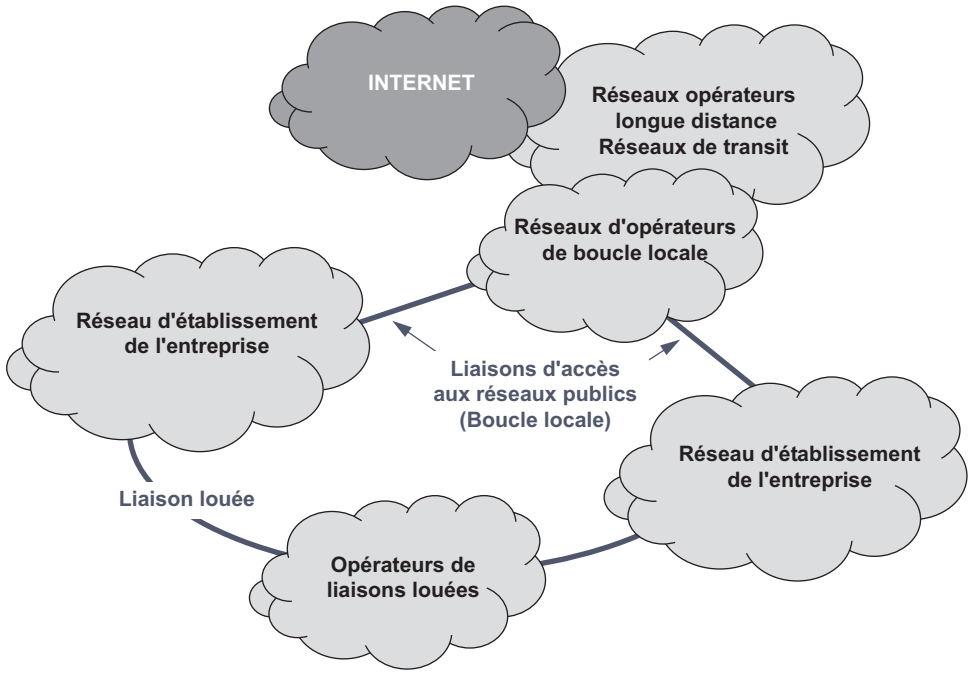


Figure 11.92 Principe du raccordement des usagers.

ressource. C'est sous le terme de dégroupage de la boucle locale que l'**ART** (Autorité de Régulation des Télécommunications) a organisé ce partage, en instituant la colocalisation des équipements actifs (figure 11.93).

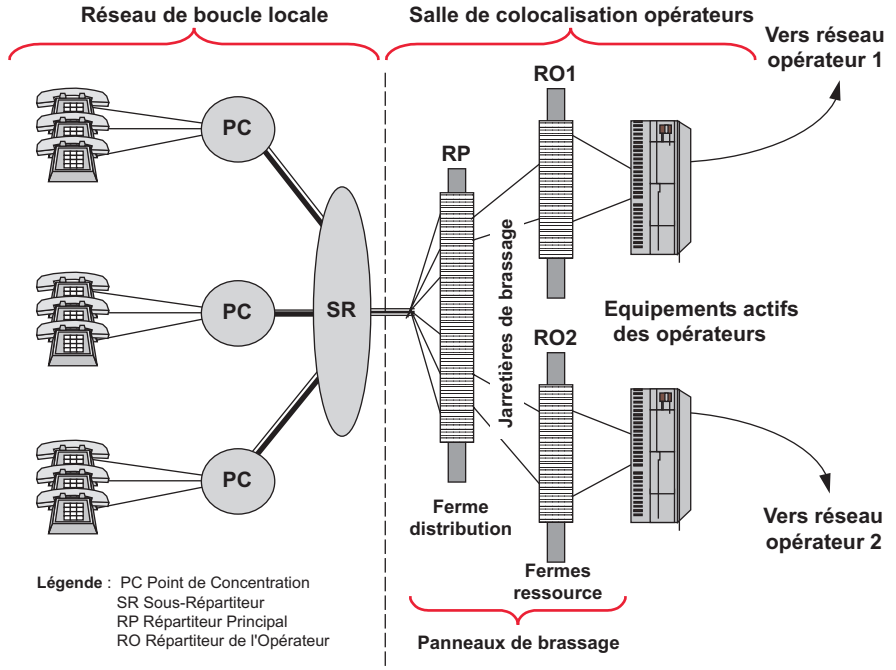


Figure 11.93 Dégroupage physique selon l'ART.

© Dunod – La photocopie non autorisée est un délit

11.3.3 La Boucle Locale Radio (BLR)

Compte tenu des coûts d'accès à l'infrastructure cuivre et/ou du coût de réalisation d'une telle infrastructure, certains opérateurs se sont tournés vers la mise en œuvre de liaisons radios (**WLL**, *Wireless Local Loop* ou Boucle Locale Radio, BLR). La BLR permet de proposer l'accès à un grand nombre d'abonnés pour un coût relativement faible, elle est particulièrement bien adaptée aux zones semi-urbaines à densité de population intermédiaire. La technologie cellulaire mise en œuvre collecte les flux et permet la diffusion. La figure 11.94 décrit un système de BLR.

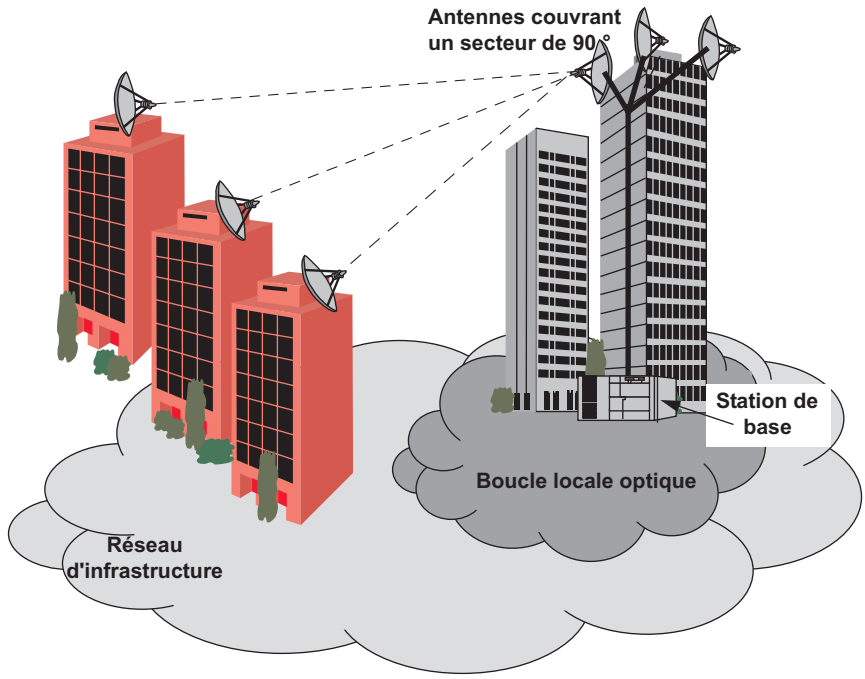


Figure 11.94 Principe de la BLR.

Utilisant une bande de fréquence de 3,5 GHz et 26 GHZ, la technologie LMDS (*Local Multipoint Distribution System*) autorise des débits de quelques Mbit/s à quelques dizaines de Mbit/s. Les cellules ont un diamètre d'environ 1 km, elles offrent un débit partagé de 5 Mbit/s dans le sens montant et de 50 Mbit/s dans le sens descendant. Cette dernière fonctionnalité devrait autoriser la distribution de programmes T.V. thématiques.

11.3.4 Les accès hauts débits

Généralités

Dans les grandes métropoles, la diffusion de programmes vidéo a largement fait appel à la fibre optique qui constitue le support idéal pour les transmissions large bande. Amener la fibre optique chez l'abonné (FTTH, *Fiber To The Home*) semble la solution idéale mais elle est trop coûteuse. Aussi, la distribution chez l'abonné final est généralement réalisée par un câble cuivre à partir d'un point de distribution commun situé dans l'immeuble (FTTB, *Fiber To The*

Basement) ou au plus près d'un groupe d'habitations (FTTC, *Fiber To The Curve*). Cependant, cette approche nécessite des travaux d'infrastructure qui ne peuvent être rentabilisés que dans les grandes métropoles. Aussi, compte tenu de la base installée, l'idée de réutiliser l'ensemble de la distribution téléphonique pour offrir, à tout abonné du réseau téléphonique commuté résidentiel ou entreprise, un accès haut débit sur une simple ligne téléphonique a conduit à rechercher de nouvelles technologies permettant d'exploiter au mieux cette infrastructure.

Les techniques DSL

La bande passante du service voix est limitée à 4 kHz, cependant la bande passante réelle de la paire torsadée dépasse le MHz. La technologie **ADSL** (*Asymmetric data rate Digital Subscriber Line*) tout en préservant la bande nécessaire au service téléphonique offre un accès haut débit à l'utilisateur final. ADSL partage la bande disponible entre le service voix (0 à 4 kHz) et deux canaux données simplex, l'un dit montant (Up) offre une bande passante de 32 à 640 kbit/s, le second (Down) un débit de 1,5 à 8,2 Mbit/s.

Les données sont transposées en fréquence selon un codage spécifique dit **DMT** (*Discrete MultiTone*) dans la bande de 25 kHz à 1,1 MHz. Le codage DMT divise chacun des spectres haut débit en sous-canaux (porteuses ou tonalités) espacés de 4,3125 kHz. Chaque sous-canal, modulé en phase et en amplitude (MAQ) codant, en principe, 8 bits dans un temps d'horloge, constitue un symbole DMT. Le nombre de bits codés par symbole dépend de l'état de la ligne. Le canal ascendant comporte 20 tonalités ou symboles DMT soit, à une rapidité de modulation de 4 kBaud (4 000 symboles DMT par unité de temps), une bande passante maximale de 640 kbit/s ($20 \cdot 8 \cdot 4\,000$). Le canal descendant est constitué de 256 sous-canaux, soit un débit maximal de 8,192 Mbit/s ($256 \cdot 8 \cdot 4\,000$). Selon les conditions de transmission sur la ligne, certains sous-canaux, dont le rapport signal sur bruit et/ou le niveau du signal sont insuffisants, peuvent être inhibés. En adaptant le nombre de bits par symbole et le nombre de sous-canaux utilisés, DMT optimise en permanence le débit en fonction de la qualité du canal de transmission par pas de 32 kbit/s (figure 11.95).

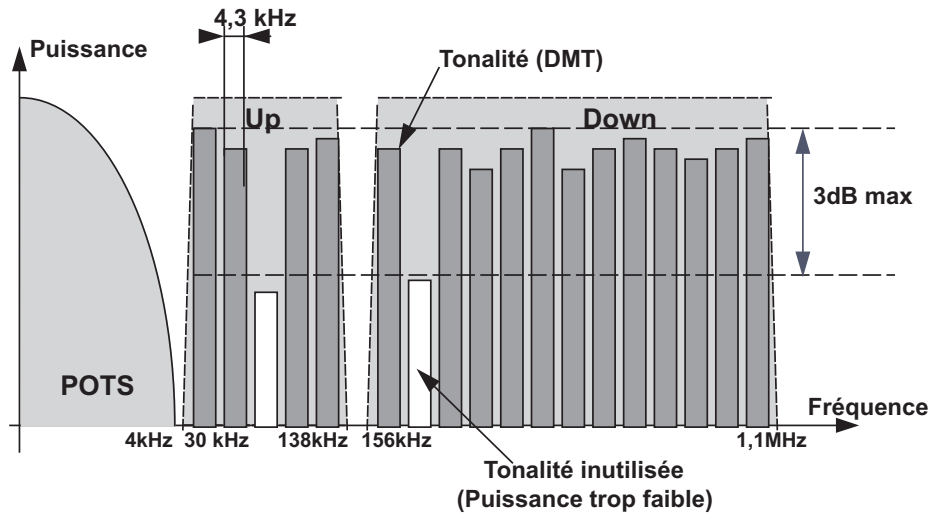


Figure 11.95 Spectre DMT utilisé dans l'ADSL.

© Dunod – La photocopie non autorisée est un délit

L'accès au réseau haut débit de l'opérateur via la ligne téléphonique nécessite l'installation d'un équipement spécifique chez l'utilisateur final qui assure la séparation des canaux : le *splitter* (séparateur vocal), ou coupleur **POTS** (*Plain Old Telephon Service*, service téléphonique traditionnel) et le modem ADSL. Le *splitter* est généralement intégré au modem. Le modem offre un accès de type Ethernet, USB ou ATM. Du côté opérateur, le **DSLAM** (*Digital Subscriber Line Access Multiplex*) est un multiplexeur statistique assurant l'interface entre les connexions utilisateurs et le réseau haut débit de l'opérateur (figure 11.96)

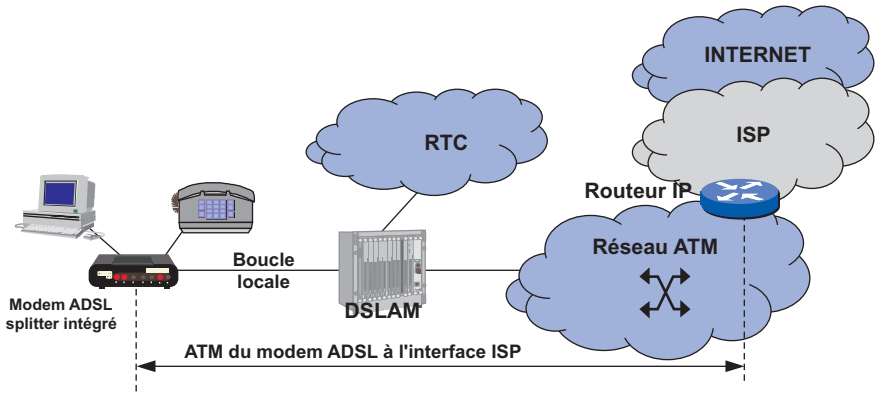


Figure 11.96 Architecture d'un réseau ADSL.

ADSL est normalisé par l'ANSI et l'ETSI. Cependant, compte tenu des investissements nécessaires au déploiement d'un réseau ADSL, les constructeurs et opérateurs ont constitué un groupe de travail, le UAWG (*Universal ADSL Working Group*), pour définir une version allégée. L'ADSL G.Lite intègre le *splitter* (séparateur de voies) au modem autoconfigurable (*Plug and Play*), limite les débits à 1,5 Mbit/s en flux montant et à 512 kbit/s en flux descendant en réduisant les sous-canaux.

Appellation	Débit descendant	Débit montant	Distance	Utilisation
ADSL	32 kbit/s à 8 Mbit/s	32 kbit/s à 1,1 Mbit/s	5,5 km	Accès professionnel à Internet Interconnexion de LAN Vidéo à la demande (VoD)
UADSL G.Lite	64 kbit/s à 1,5 Mbit/s	32 kbit/s à 512 kbit/s	5,5 km	Accès résidentiel à Internet
SDSL	1,54 Mbit/s (T1) 2,048 Mbit/s (E1)	1,54 Mbit/s (T1) 2,048 Mbit/s (E1)	6,5 km	Interconnexion de LAN Serveur Internet Vidéoconférence
IDSL	144 kbit/s à 1,5 Mbit/s	32 kbit/s à 512 kbit/s	11 km	Accès RNIS
VDSL	13 à 52 Mbit/s	1,5 à 2,3 Mbit/s	1,2 km	Accès Internet, VoD TV haute définition
HDSL	1,5 Mbit/s (T1) 2,048 Mbit/s (E1)	1,5 Mbit/s (T1) 2,048 Mbit/s (E1)	4,5 km	Accès professionnel E1 Raccordement PABX Interconnexion de LAN

Figure 11.97 Les différentes technologies xDSL.

Compte tenu de l'intérêt économique des techniques DSL, d'autres solutions ont été développées pour raccorder à moindres frais les usagers aux réseaux des opérateurs. Le tableau de la figure 11.97 présente succinctement ces différentes versions.

11.4 CONCLUSION

Le transport de flux de natures différentes impose aux réseaux des exigences en termes de qualité de service. Ces exigences sont prises en compte dans l'ATM par la notion de classe de service, dans IP avec l'intégration de DiffServ et dans les réseaux locaux par l'approche 802.1p. La pluralité de normes et de protocoles d'origines différentes ne simplifie pas la tâche. La qualité de service sera l'enjeu principal des réseaux des années à venir (figure 11.98).

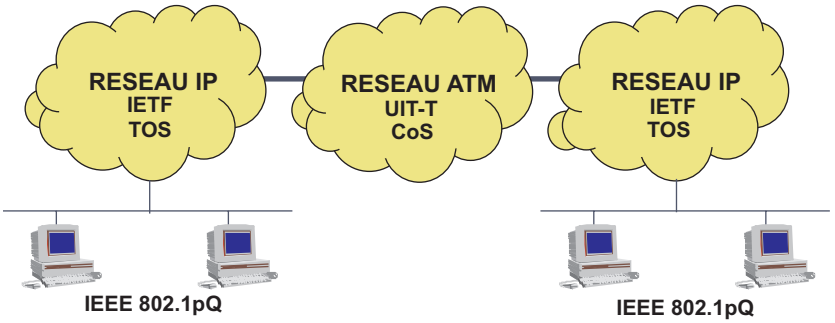


Figure 11.98 Problématique de la QoS de bout en bout.

© Dunod – La photocopie non autorisée est un délit

EXERCICES

Exercice 11.1 SDH/PDH

Quels sont les principaux avantages de la hiérarchie SDH vis-à-vis de la hiérarchie PDH ?

Exercice 11.2 Paquet d'appel X.25

Reconstituez le paquet d'appel émis par une station devant se connecter sur un ETTD distant. L'adressage est du type X.121, l'ETTD est relié au réseau par une LS (valeur 1) : ligne 89 sur le commutateur 1 du département de la Seine (75). Les services complémentaires suivants seront invoqués :

– facturation à l'appelé ;

– GFA valeur locale 3 ;

– négociation de la taille des paquets, 64 en émission, 128 en réception ;

– négociation de la taille fenêtre, 2 en réception, 7 en émission.

Nous supposerons que le réseau n'utilise qu'une numérotation des paquets modulo 8. On admettra que l'appel est le premier émis par l'ETTD dont l'abonnement comporte 20 CV. L'opérateur utilise un format d'adresse du type :

<mode d'accès (1), département (2), commutateur (2), ligne abonné (4)>

Les valeurs entre parenthèses indiquent la longueur du champ en quartets.

Exercice 11.3 Dialogue X.25

À l'aide de la trace du niveau physique représentée figure 11.99, reconstituez et commentez le dialogue entre l'ETTD et le réseau.

Ligne	Origine	Champ
1	ETCD	7E 01 0F 68 B9 7E
2	ETCD	7E 01 0F 68 B9 7E
3	ETCD	7E 01 0F 68 B9 7E
4	ETTD	7E 01 3F EB 7F 7E
5	ETCD	7E 01 73 83 5E 7E
6	ETCD	7E 03 00 10 00 FB 07 A4 EA 6F 7E
7	ETTD	7E 03 21 A4 56 7E
8	ETTD	7E 01 20 10 00 FF 8D 06 7E
9	ETCD	7E 01 21 14 98 7E
10	ETTD	7E 01 22 10 03 0B 09 19 20 20 59 30 02 01 01 C4 01 00 67 89 7E
11	ETCD	7E 01 41 12 14 7E
12		7E 03 42 10 03 0F 70 A9 7E
13	ETTD	7E 03 41 A2 DA 7E
14	ETTD	7E 01 44 10 03 00 E0 00 00 01 00 20 08 00 10 00 C2 00 50 49 00 08 08 00 00 00 50 52 00 08 00 00 0E 60 50 6B 00 14 02 00 00 23 01 00 10 01 18 50 C9 05 00 00 00 00 01 24 7E

Figure 11.99 Trace X.25.

Exercice 11.4 Définition d'un protocole

Vous avez été recruté par un nouvel opérateur afin de participer à la conception de son réseau national. Après avoir défini la topologie du réseau, il vous reste à préciser l'aspect protocolaire. À cet effet, on vous demande de réfléchir aux points suivants :

a) Sachant que le temps théorique de transfert d'un message de longueur L en commutation de paquets est donné par la relation :

$$Tp = \frac{L + pH}{D}\left(1 + \frac{N}{p}\right)$$

Où L est la longueur du message en bits, p le nombre de paquets, H la taille en bits des données protocolaires, N nombre de nœuds traversés (nœuds origine et destination non compris) et D débit en bit/s.

On vous demande de déterminer la taille optimale de l'unité de données (temps de traversée du réseau minimale), pour cela on formule les hypothèses suivantes :

– Tous les clients sont raccordés via une interface 802.3, on admettra que la longueur du message utilisera au maximum les capacités de transfert du réseau local (MTU de la trame 802.3, 1 500 octets).
– La topologie du réseau WAN est telle qu'un paquet traverse en moyenne 3,25 nœuds.
– Les données de services du protocole WAN seront limitées à 5 octets.
– On ne retiendra que la valeur entière du résultat final.

b) Le réseau offrira un service en mode connecté, on envisage d'utiliser un contrôle de flux du type Stop and Wait. C'est-à-dire, que dès qu'un nœud reçoit un paquet saturant, il envoie à la source une demande d'arrêt d'émission. Le contrôle de flux sera instauré, d'une part entre le nœud client et le nœud d'accès au réseau (contrôle de flux à l'interface usager) et, d'autre part entre les nœuds du réseau (deux à deux). Est-il réaliste d'instaurer de tels mécanismes sachant que :

1) En interne au réseau
   – La distance moyenne séparant 2 nœuds est de 100 km.
   – Le débit interne du réseau de 622 Mbit/s.
   – La vitesse de propagation des données sera supposée être de 2.10^8 m/s.
2) À l'interface usager
   – La distance maximale de la liaison d'abonnée est estimée à 20 km
   – Le débit maximal offert à l'usager est de 2,048 Mbit/s

On admettra que le temps de traitement par les nœuds des unités de données est négligeable.

c) Combien de connexions simultanées (CV) le réseau peut accepter si on a réservé, dans les 5 octets d'en-tête, 28 bits à l'espace d'adressage ?

d) On admet que **chacun** des liens est affecté d'un taux d'erreur binaire de Teb = 10^{-9}

© Dunod – La photocopie non autorisée est un délit

– Quelle est la probabilité qu'un paquet arrive à destination sans erreur (9 décimales) ?

– Avec au moins 1 bit erroné (9 décimales) ?

e) Compte tenu de la probabilité d'erreur relativement importante. Est-il possible de garantir, même à charge constante, aux utilisateurs un temps de traversée du réseau borné et une gigue nulle ?

f) Vous envisagez des accès via le réseau téléphonique. Quel sera le débit maximal possible par ce moyen d'accès compte tenu des données suivantes :

– Le rapport signal à bruit moyen du RTC est de 10^3.

– Le RTC est équipé de filtres (bande passante téléphonique normalisée).

Vous comptez utiliser des modems dont les différents instants significatifs sont repérés à 0, $\pi/4$, $\pi/2$, $3\pi/4$, π, $5\pi/4$, $3\pi/2$, $7\pi/4$, chaque vecteur pouvant être défini à + 3V ou + 1V. Est-ce réalisable ?

Exercice 11.5 Protocole ATM

Pourquoi, l'utilisation de la liaison virtuelle identifiée VPI/VCI 0/0 est-elle interdite pour transmettre des unités de données d'administration, de signalisation ou usagers ?

Exercice 11.6 Qualité de service

La notion de classes de service d'ATM est relativement complexe à mettre en œuvre, les systèmes à priorité sont plus faciles à implémenter. Quel est, d'après vous, le meilleur système pour garantir une qualité de service, notamment pour les flux isochrones ?

Exercice 11.7 Rendement protocolaire

1) Sur votre réseau, vous désirez accueillir des stations nomades, à des fins de sécurité absolue vous avez décidé de développer un modem propriétaire. Sachant que la bande passante téléphonique pratique est plus grande que la bande passante théorique, vous comptez utiliser la bande de 200 à 3 800 Hz. Cependant, ces caractéristiques n'étant pas garanties en tout point du réseau téléphonique, vous décidez de développer votre modem sur le même modèle qu'ADSL. C'est-à-dire utiliser un ensemble de sous-porteuses, chacune transportant 128 symboles (1 symbole égal 1 octet) et appelée tonalité. Sachant que chaque tonalité occupera un spectre de fréquence de largeur 100 Hz et que, pour éviter les interférences, les spectres de chaque tonalité seront écartés de 20 Hz (bande de garde).

a) Quelle est la largeur de bande occupée par une tonalité ?

b) Combien de tonalités pourront être utilisées simultanément ?

c) Dans cette hypothèse quel est le débit maximal du système ?

2) À l'instar d'ADSL, pour assurer l'adaptation à la ligne le système n'utilisera pas les tonalités dont le niveau sera atténué de 3 dB et plus par rapport à la tonalité la mieux transmise. Pour tester votre modem, vous relevez la bande passante de votre ligne test. Le résultat des mesures est donné par le tableau ci-dessous (figure 11.100).

Tonalité	Niveau en mW	Tonalité	Niveau en mW
1	8	16	8
2	7	17	8
3	9	18	8
4	8	19	9
5	4	20	8
6	3	21	8
7	6	22	9
8	6	23	9
9	6	24	9
10	7	25	8
11	8	26	8
12	6	27	7
13	5	28	6
14	4	29	5
15	4	30	4

Figure 11.100 Bande passante (Puissance/Fréquence) de la ligne.

a) Quelle est la puissance de la tonalité la mieux reçue ?

b) Quelle est la puissance minimale des tonalités susceptibles d'être validées par le système ?

c) Dans ces conditions, quel est le nombre de tonalités qui seront validées par le système ?

d) Quel sera alors le débit binaire réel du modem ?

3) Sachant que :

– les messages sont issus d'une trame Ethernet remplie au maximum de sa capacité de transport (MTU d'Ethernet),

– le protocole réseau est TCP/IP (aucune option n'est invoquée),

– le transfert se fait en mode cellules ATM, nous supposerons que le datagramme IP est directement encapsulé dans la couche d'adaptation AAL5,

– l'AAL5 fait du bourrage pour que les données soient segmentées en un nombre entier de cellules complètes et utilise 8 octets pour gérer le protocole.

On vous demande :

a) Quel est le nombre minimal et maximal d'octets de bourrage que la couche AAL5 est susceptible d'introduire ?

b) Compléter la figure 11.101, en remplaçant les X par la valeur en octets du champ.

c) Quel est le nombre de cellules ATM qui seront constituées ?

© Dunod – La photocopie non autorisée est un délit

d) Quel est le rendement du protocole (rapport entre le nombre de bits utiles et le nombre de bits transmis) ?

e) Quel est alors le taux de transfert d'information (bit/s) ?

f) En supposant un taux d'erreur de 10^{-6} quel est le taux de transfert d'information réel (bit/s) ?

g) Quel est le rendement global du système (TTI/Possibilité du modem)

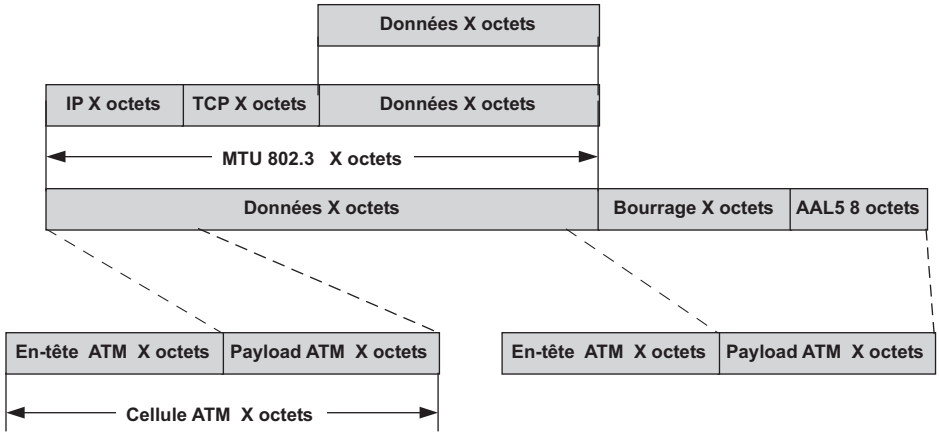


Figure 11.101 Encapsulation de données dans ATM.

Exercice 11.8 Évolution de l'encapsulation d'IP

Veuillez compléter le tableau ci-dessous (figure 11.102) qui résume les différentes possibilités d'encapsulation du protocole IP pour en assurer le transport sur un réseau WAN.

Type d'encapsulation	Mise en œuvre	Caractéristiques
IP/ATM/SDH/WDM		
IP/SDH/WDM		
IP/WDM		

Figure 11.102 Encapsulation IP.

Chapitre **12**

Les réseaux locaux Ethernet, CSMA/CD, Token Ring, VLAN...

12.1 INTRODUCTION

12.1.1 Définition

L'évolution générale des systèmes d'information et des moyens d'y accéder ont engendré une modification significative des méthodes de travail. D'individuel, le travail est devenu collectif. Les besoins d'information et de communication dans le groupe de travail ont été décuplés. Le micro-ordinateur et le réseau local sont à l'épicentre de cette mutation (figure 12.1).

Figure 12.1 Le réseau local et le micro-ordinateur épicentre du travail collectif.

Un réseau local est un ensemble de moyens autonomes de calcul (micro-ordinateurs, stations de travail ou autres) reliés entre eux pour s'échanger des informations et partager des ressources matérielles (imprimantes, espace disque...) ou logicielles (programmes, bases de

données...). Le terme de réseau local (**LAN**, *Local Area Network*) qui définit un LAN comme un système de communication entre unités centrales sur une étendue géographique limitée est restrictif. Faisant abstraction de la notion d'étendue géographique, le terme de réseau local d'entreprise (**RLE**) semble mieux approprié.

12.1.2 Distinction entre réseau local et informatique traditionnelle

Entre un terminal passif, par exemple un terminal Telnet, en informatique traditionnelle centralisée, et un poste client d'un réseau local, le plus souvent un micro-ordinateur, la différence essentielle concerne la localisation des traitements et de la politique d'accès (figure 12.2).

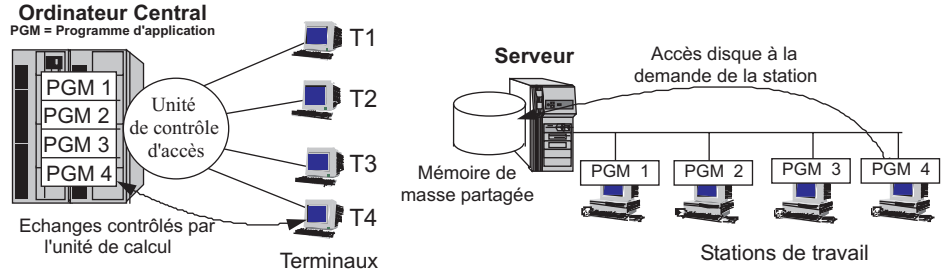


Figure 12.2 Localisation de la puissance de calcul.

Un terminal passif ne dispose d'aucune puissance de calcul, les diverses applications partagent le temps CPU de l'ordinateur central. Celui-ci contrôle le traitement et organise les accès (politique d'accès centralisé : *polling/selecting* ou relation maître/esclave). Un poste client (**station**) d'un réseau local dispose d'une puissance de calcul autonome, le programme principal s'exécute en local, il n'émet des requêtes au serveur que pour utiliser les ressources partagées et offertes par ce dernier. Il n'y a pas de subordination entre les différents constituants du réseau. Dans ces conditions, ceux-ci partageant le même média, une discipline d'accès (**protocole d'accès**) doit être implémentée dans chaque unité (politique ou contrôle d'accès décentralisé).

Un réseau local distingue deux types de machines, celles qui offrent des ressources en partage : les serveurs, et celles qui utilisent ces ressources : les postes clients, postes de travail ou stations. Dans les réseaux locaux de la dernière génération toutes les machines peuvent offrir des ressources en partage et utiliser celles offertes par les autres stations du réseau. Ce type de réseau est désigné sous le nom de *peer to peer* ou poste à poste ou encore d'égal à égal. En fait, dans les réseaux importants, une machine dédiée aux fonctions traditionnelles de serveur subsiste. Celle-ci assure la gestion des utilisateurs, la sécurité d'accès, la distribution des logiciels...

12.1.3 Réseaux locaux et accès aux systèmes traditionnels

Pour l'utilisateur, la distinction entre les systèmes est masquée. Une station d'un réseau local peut donner accès aux applications d'un ordinateur central (mini ou *mainframe*). Le programme client émule alors un terminal de l'autre système. L'une des stations assure les fonctions de passerelle vers le système central (figure 12.3).

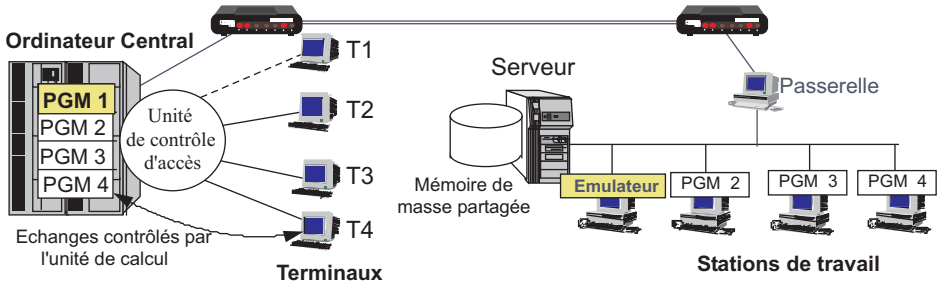


Figure 12.3 L'accès aux moyens de calcul traditionnels via un réseau local.

Dans la figure 12.3, une station du réseau local exécute un programme qui émule un terminal dédié du système centralisé (**émulation de terminal**) et permet l'accès au PGM1 qui se déroule sur l'ordinateur central. Une autre machine du réseau local, dite passerelle (*gateway*), permet l'accès à la machine centrale qui peut être locale ou distante, c'est un concentrateur d'accès. Sur l'ordinateur central, un programme d'émulation simule un dialogue local entre le terminal et l'application. C'est ce programme d'émulation qui contrôle le dialogue avec l'application PGM1. L'émulateur local convertit, vis-à-vis de l'utilisateur, le poste de travail en terminal passif dédié.

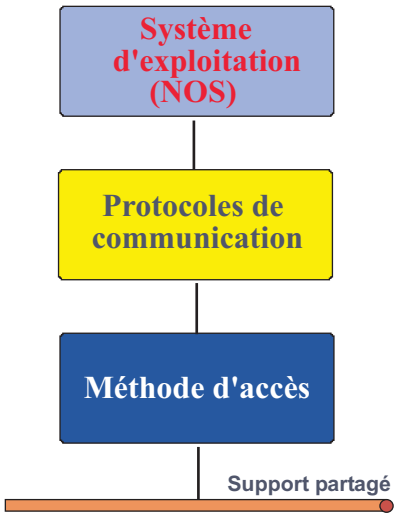


Figure 12.4 Principaux constituants d'un nœud de réseau local.

12.1.4 Constituants d'un réseau local

Architecture informatique dédiée à l'échange d'information et au partage de ressources physiques, un réseau local est essentiellement constitué par (figure 12.4) :

– un câblage reliant les différents nœuds selon une certaine topologie ;
– une méthode d'accès au support pour assurer son partage ;
– une méthode d'adressage pour identifier chaque nœud ;
– un ensemble cohérent de protocoles (pile) pour permettre la communication ;

© Dunod – La photocopie non autorisée est un délit

– un système d'exploitation spécifique (**NOS**, *Network Operating System*) capable de prendre en charge les périphériques distants partagés et d'en contrôler l'utilisation (administration et sécurité) ;
– un ensemble de programmes utilisant les ressources mises en commun.

Pour assurer l'intégralité de ces fonctionnalités, il a fallu adapter l'architecture du modèle de référence de l'ISO. L'architecture OSI répond à l'interconnexion de systèmes en mode point à point, alors que les réseaux locaux partagent un support unique en mode diffusion. Les couches hautes du modèle qui gèrent la communication restent applicables aux réseaux locaux. Cependant, les couches basses qui organisent l'accès au support devront être adaptées (figure 12.5) :

– afin de décrire une interface indépendante du support, la couche physique a été scindée en deux. La sous-couche basse (sous-couche **PMD**, *Physical Medium Dependent*) assure le transfert des données (bits) sur une gamme de supports variés : câble coaxial, paire torsadée, fibre optique, réseaux sans fil. La sous-couche supérieure (**PMI**, *Physical Medium Independent*) est chargée de la détection de présence d'un signal, du codage et de la récupération de l'horloge (synchronisation) ;
– la couche liaison a, aussi, été divisée en deux. La sous-couche la plus basse contrôle l'accès partagé au support (sous-couche **MAC** ou *Medium Access Control*) et le contrôle d'erreur, la sous-couche supérieure (sous-couche **LLC**, *Logical Link Control* ou Contrôle du lien logique) remplit les fonctions traditionnellement dévolues à la couche liaison (établissement d'un lien logique).

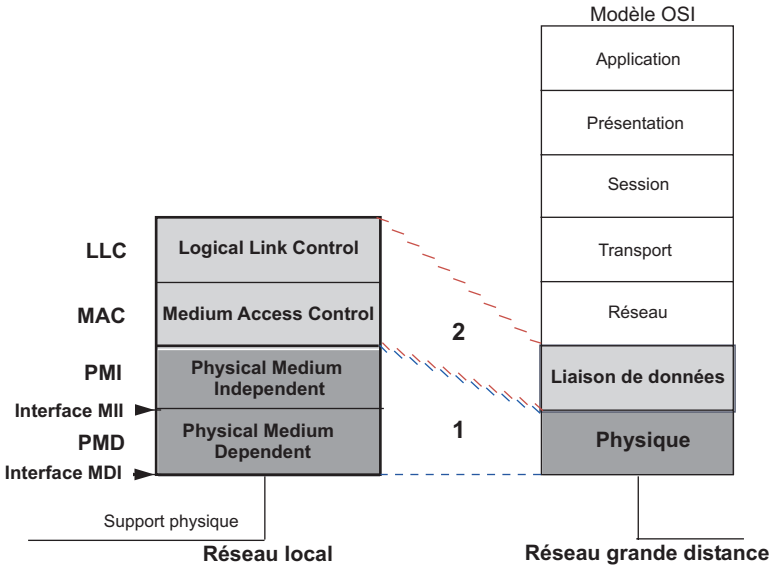


Figure 12.5 Les couches 1 et 2 dans les réseaux locaux.

Deux problèmes importants sont à résoudre : l'adressage des machines connectées et l'analyse des commandes. Le modèle de référence définit l'adressage des systèmes au niveau réseau (couche 3). Cette adresse détermine le point de raccordement de l'hôte dans le réseau étendu.

Si, dans les réseaux locaux, ce système d'adressage était maintenu tel quel, chaque message circulant sur le réseau provoquerait, dans chaque poste raccordé, une interruption processeur. Le processeur examinerait l'adresse pour s'apercevoir que le message ne lui était pas destiné, ce qui grèverait gravement les performances de toutes les stations du réseau. Dans les réseaux locaux, il n'y a aucun besoin de localisation, il suffit de distinguer une interface parmi toutes celles raccordées localement sur un même réseau. Chaque interface sera distinguée par un numéro, appelé adresse physique ou adresse MAC (adressage à plat). Le message ne sera transmis aux couches supérieures que s'il concerne l'interface du nœud destinataire.

Sur une machine connectée en réseau local, les différentes commandes peuvent être adressées soit au système local soit à un système distant. Il est donc nécessaire de distinguer ces deux types d'appel. Une couche fonctionnelle dite « redirecteur », spécifique au système d'exploitation réseau, a pour rôle de diriger les appels vers le système cible. La notion de redirecteur[1] n'est pas définie par l'ISO. Cependant, on peut admettre qu'elle se situe au niveau de la couche présentation. La figure 12.6 matérialise cette architecture.

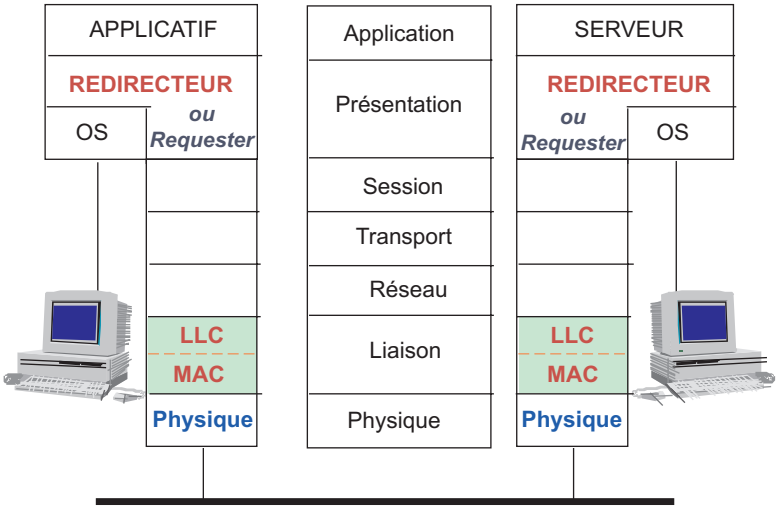


Figure 12.6 Architecture générale des réseaux locaux.

12.1.5 Les réseaux locaux et la normalisation

Devant la diversité des besoins et des produits proposés, **l'IEEE** (*Institute of Electrical and Electronic Engineers*) a créé le groupe de travail 802 (février 1980) chargé de définir des standards (Standards 802.x). En 1988, l'ISO a repris la plupart de ces standards pour les normaliser et en faire des normes internationales (série IS 8802.*x*).

Cependant, l'IEEE poursuit son travail de normalisation. Le groupe 802 est divisé en sous-groupes de travail, chacun chargé d'un domaine particulier. Il s'agit des comités suivants dont la structure reflète les normes spécifiées :

1. Le redirecteur, désignation Microsoft, est couramment appelé *requester* ou *shell* chez Novell.

© Dunod – La photocopie non autorisée est un délit

– le Comité 802.1 définit l'architecture générale des réseaux et détermine le format d'adressage, les techniques d'interconnexion et d'administration ;
– le Comité 802.2 précise les fonctionnalités de la couche liaison de données (sous-couche **LLC**, *Logical Link Control)*. Il a défini trois types de services : **LLC1** (service en mode non connecté), **LLC2** (service en mode connecté proche d'HDLC) et **LCC3** (service en mode non connecté mais avec acquittement) ;
– les Comités 802.3 à 802.6 et 802.11 à 802.14 spécifient les méthodes d'accès (sous-couche MAC) et les couches physiques correspondantes.
– les Comités 802.7 et 802.8 assurent la coordination des autres comités dans les domaines de large bande (802.7) et de la fibre optique (802.8) ;
– le Comité 802.11 étudie les réseaux sans fils (*Wireless LAN*).

La figure 12.7 représente l'architecture normalisée des réseaux locaux.

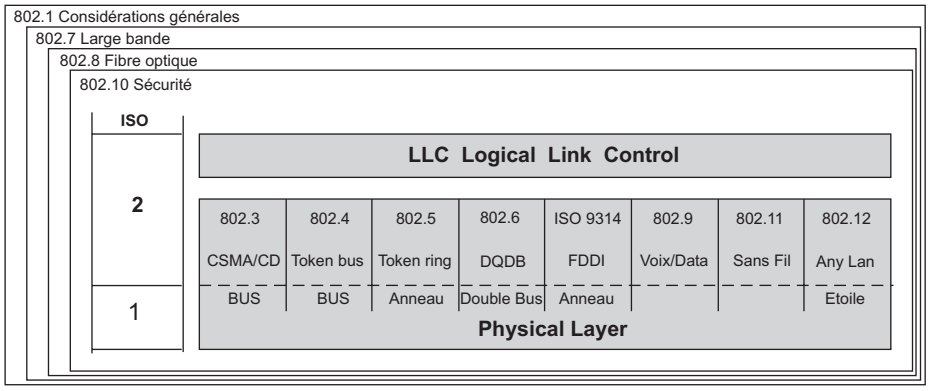


Figure 12.7 Les réseaux locaux et la normalisation.

12.2 ÉTUDE SUCCINCTE DES DIFFÉRENTES COUCHES

Ce paragraphe se propose d'étudier de manière générique les couches 1 et 2 des réseaux locaux. L'algorithme d'accès au support sera examiné lors de l'étude de la couche MAC de chaque type de réseau.

12.2.1 La couche physique

La couche physique spécifie les modes de raccordement (topologie et câblage), les niveaux électriques et le codage des informations émises.

Les topologies

➤ Topologie et méthodes d'accès

La topologie d'un réseau décrit la manière dont les différents composants du réseau sont reliés. Les réseaux locaux utilisent les topologies de base comme le bus, l'anneau et l'étoile (figure 12.8) ou des combinaisons de celles-ci (étoile de bus, grappe d'étoiles...).

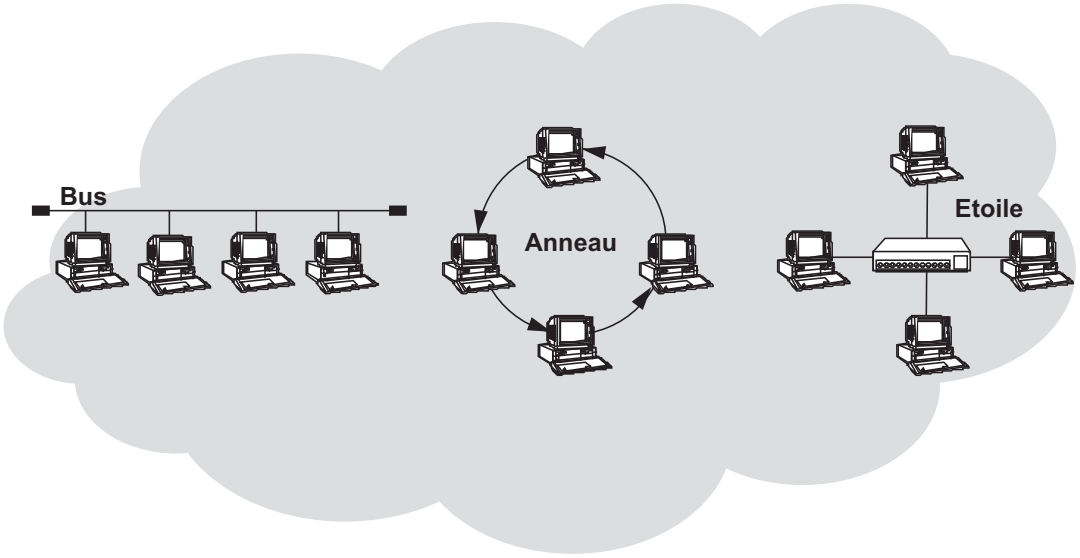


Figure 12.8 Les topologies de base.

Sur un bus, les unités sont au même niveau hiérarchique, les messages sont reçus par l'ensemble des stations (diffusion). Le système n'étant pas hiérarchisé, une station peut accéder au support à tout moment. Ce mode d'accès n'interdit pas à deux stations d'émettre en même temps, les messages sont alors altérés : il y a collision ou contention. Pour résoudre ce problème, des règles d'accès au support doivent être fixées :

– la station vérifie, avant d'émettre, qu'aucune autre n'est en émission (écoute du support), cette méthode d'accès est utilisée par les réseaux IEEE 802.3 appelés « **Ethernet**[2] » ;
– selon une autre méthode, chaque station se voit successivement attribuer le droit d'émettre par un message particulier : le *token* ou jeton. Chaque station qui reçoit le jeton l'adresse à la suivante (jeton adressé). Cette méthode est utilisée dans les réseaux industriels de type IEEE 802.4 ou **Token Bus**.

L'anneau est un cas particulier d'une liaison multipoint, il implique une circulation unidirectionnelle des messages. Le message est relayé par toutes les stations jusqu'à son destinataire. Dans ce type de topologie le droit d'émettre (jeton) est transmis à la station qui suit physiquement celle qui le détient (jeton non adressé). Cette méthode d'accès est mise en œuvre dans le réseau IEEE 802.5 ou **Token Ring**.

Les topologies en étoile sont une variante des liaisons point à point, ils constituent *n* liaisons point à point autour d'un concentrateur. Ce dernier peut n'être qu'un répéteur (hub du réseau IEEE 802.3 10 base T) ou participer activement à la distribution de l'accès au support (IEEE 802.12 ou Any Lan). Dans ce dernier cas, une station qui désire émettre formule une demande au concentrateur qui lui alloue ou non le droit d'émettre.

2. Ethernet est un nom de marque déposé par Xerox. Ce nom est passé dans le langage courant et désigne les réseaux de type CSMA/CD.

© Dunod – La photocopie non autorisée est un délit

➤ Topologie physique et topologie logique

Dans les réseaux locaux, on distingue la topologie physique qui indique comment les différentes stations sont physiquement raccordées (câblage), de la topologie logique qui décrit comment est distribué le droit d'émettre.

En diffusant les messages sur tous ses ports, l'élément actif appelé hub[3] (topologie étoile) émule un bus. La station « A » de la figure 12.9 émet un message, celui-ci est transmis par son hub de raccordement à toutes les stations connectées sur le même hub et au hub de niveau supérieur pour que celui-ci assure la diffusion du message à l'ensemble des stations constituant le réseau (réseau IEEE 802.3 10 base T).

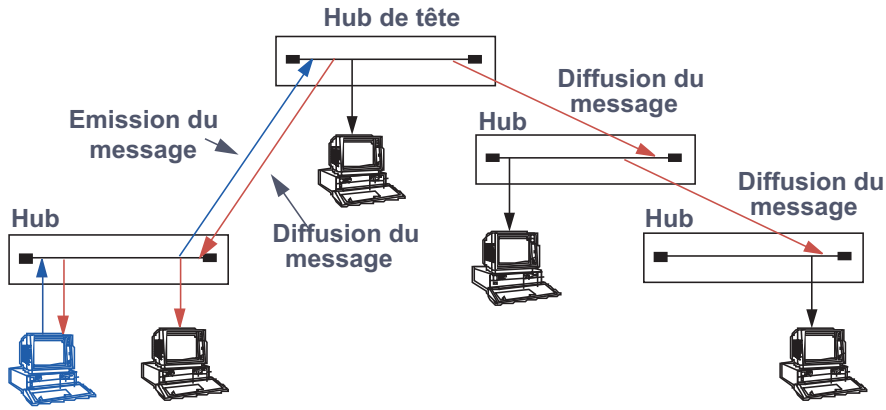


Figure 12.9 Étoile physique, bus logique.

Dans une topologie en anneau, chaque station participe à la diffusion du message et à sa régénération. L'arrêt d'une station interrompt ce mécanisme. Pour pallier ceci, les stations sont raccordées physiquement à un concentrateur d'accès (**MAU**, *Multiple access Unit*) dont le rôle est de détecter les stations hors service et de court-circuiter leur raccordement (*by-pass*). Le raccordement des stations assure le prolongement de l'anneau à l'extérieur du MAU, il est désigné sous le terme de lobe. Ce type de configuration : anneau logique/étoile physique est utilisé dans les réseaux IEEE 802.5 ou Token Ring (figure 12.10).

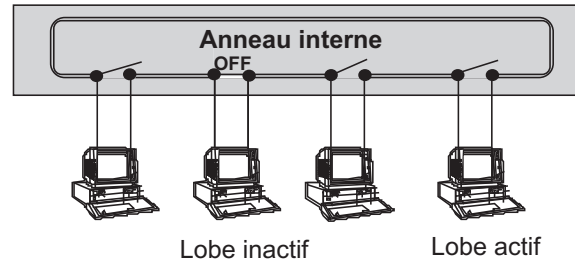


Figure 12.10 Étoile physique, anneau logique.

3. Un hub n'est ni réellement un concentrateur, ni seulement un répéteur. Ces termes, couramment utilisés pour désigner le hub sont imprécis. Dans la suite de cet ouvrage nous n'utiliserons que le terme de hub.

Le câblage

➤ Généralités

Les réseaux locaux utilisent tous les types de support : les câbles cuivre (coaxial, paires torsadées), les supports optiques (fibre optique) et les supports hertziens (réseaux sans fil). Le câble coaxial a longtemps été utilisé (réseaux de type Ethernet), mais il est aujourd'hui remplacé par la paire torsadée moins chère et plus facile d'installation. La fibre optique est essentiellement réservée aux réseaux haut débit et à l'interconnexion de réseaux. La figure 12.11 présente une synthèse des différentes caractéristiques des câbles.

Type de câble	Immunité électromagnétique	Débit courant	Distance	Utilisation
Coaxial	Bonne	10 Mbit/s	2 500 m par brin de 500 m	Ethernet, en environnement perturbé ou confidentiel.
Paires torsadées UTP	Faible	10 à 100 Mbit/s	100 m d'un élément actif	Ethernet sur paires torsadées.
Paires torsadées FTP	Moyenne	10 à 100 Mbit/s	100 m d'un élément actif	Ethernet paires torsadées, Token Ring.
Fibre optique	Excellente	100 à 155 Mbit/s	Une centaine de km	FDDI

Figure 12.11 Les différents câbles mis en œuvre dans les réseaux locaux.

➤ Le précâblage d'immeuble

Le développement intensif des postes de travail en réseau local a révélé des problèmes liés au câblage. Les réseaux locaux ont tous, aujourd'hui, une topologie physique en étoile, d'où l'idée de réaliser, dans les immeubles de bureaux, un précâblage (figure 12.12). Un système de précâblage doit :

– assurer que tout poste de travail ne sera qu'à quelques mètres d'une prise informatique ou téléphonique ;

– être indépendant du type de réseau et de la topologie réseau choisis.

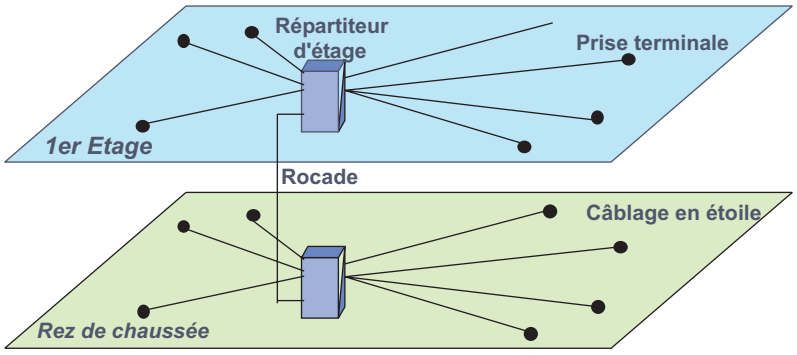


Figure 12.12 Structure générale d'un précâblage d'immeuble.

© Dunod – La photocopie non autorisée est un délit

Les principaux systèmes sont **l'ICS** (*IBM Cabling System*), le **BCS** (*Cabling System*), *l'Open Link* de **DEC** et le **PDS Systimax d'AT&T**. Ces systèmes ont en commun l'utilisation de la paire torsadée et une topologie physique en étoile. Le cœur du câblage est constitué de panneaux, dits **panneaux de brassage**, qui permettent, à l'aide de jarretières, de réaliser la connexion des postes de travail selon la topologie requise par le réseau. Ces systèmes diffèrent essentiellement par le type de câble utilisé (UTP, FTP). Le débat sur les différentes impédances s'est aujourd'hui tari au profit du câble 100 Ω. La dernière version de la norme ISO (IS 11 801 du 23/10/2002) déclasse le 120 Ω en classe D.

Les câbles sont classés en catégorie selon les spécifications auxquels ils répondent : atténuation, bande passante, *Next*... (figure 12.13).

Catégorie	Classe	Impédance	Fréquence Max	Applications
3	C	100-120 Ω	16 MHz	Token Ring 4 Mbit/s 10 Base T Fast Ethernet 100 VG Any Lan 100 Base T4
4	D	100 Ω	20 MHz	Token Ring 16 Mbit/s
5	D	100 Ω	100 MHz	100 Base Tx ATM 155 Mbit/s ATM 622 Mbit/s (Draft) 1 000 Base T (Cat 5E)
6	E	100 Ω	250 MHz	1 000 Base Tx ATM 1,2 Gbit/s (Draft)

Figure 12.13 Les catégories de paires torsadées.

Le câble catégorie 5 est aujourd'hui le plus installé. Cependant, ses performances sont limitées. Dans l'attente de la catégorie 6, un câble aux performances améliorées a été défini : la catégorie 5e (étendu). Devant l'importance et les enjeux économiques du câblage, l'ISO tente, actuellement, d'édicter une normalisation : le **GCS** (*Generic Cabling Standard*). La figure 12.14 représente les différents constituants participant à la réalisation physique d'un réseau local. Un local technique (local de brassage) abrite une armoire technique ou armoire de brassage. Celle-ci accueille les éléments actifs (hub, MAU), parfois les serveurs (salle réseau) mais surtout les panneaux de brassage. Le précâblage consiste à « tirer » des câbles entre le panneau de brassage et les prises murales. Pour raccorder une station, il suffit de connecter celle-ci à la prise murale par un cordon dit de raccordement. À l'autre extrémité, au panneau de brassage, on tire une jarretière (cordon de raccordement ou de brassage) entre la prise RJ45 correspondant à la prise murale et un port de l'élément actif. Chaque point de raccordement peut constituer une désadaptation d'impédance et engendrer des ondes stationnaires. Il est impératif de veiller à la qualité de tous ces éléments et de vérifier qu'ils sont qualifiés pour le type de réseau mis en œuvre.

Les seules contraintes d'installation de la paire torsadée concernent la distance minimale à respecter avec les sources de rayonnement électromagnétique (distribution courant fort, tubes fluorescents, machinerie électrique...). Par exemple, le cheminement parallèle de câbles courant faible et courant fort doit respecter un écartement minimal de 5 cm si le cheminement est inférieur à 10 m, 15 cm jusqu'à 30 m et 30 cm au-delà. Le rayon de courbure des câbles

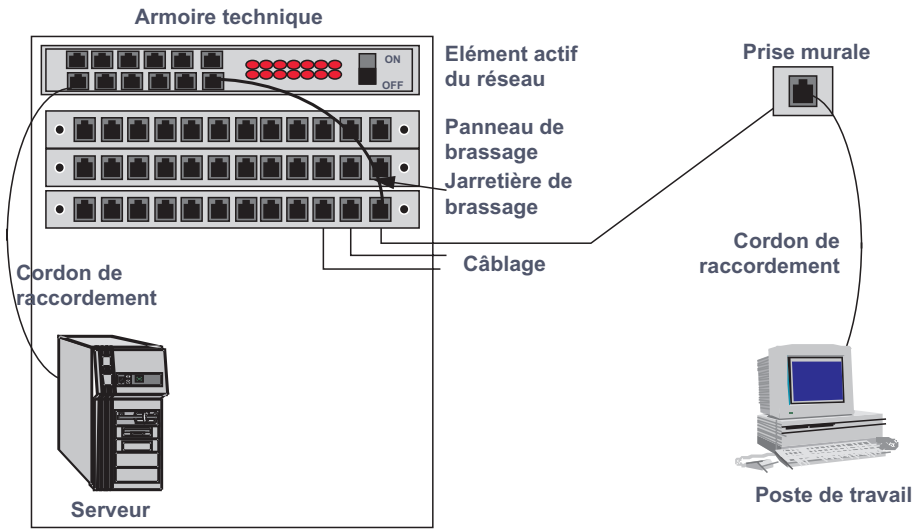


Figure 12.14 Constituants physiques d'un réseau local.

(1,5 fois le diamètre du câble) et la longueur maximale de « détorsadage » des paires pour réaliser la connectique (1,5 cm) sont des points à examiner lors de la recette d'un câblage.

12.2.2 La sous-couche MAC

La sous-couche **MAC** (*Medium Access Control*) a pour mission essentielle de gérer l'accès au support physique, elle règle les problèmes d'adressage (adresse MAC) et effectue un contrôle d'erreurs (**FCS**, *Frame Check Sequence*).

Les méthodes d'accès, généralités

Ce sont les méthodes d'accès qui distinguent les différents types de réseau et déterminent leurs performances dans tel ou tel environnement. Deux méthodes dominent le monde des réseaux locaux : les méthodes aléatoires ou à contention, mises en œuvre dans les réseaux de type Ethernet, et les méthodes à réservation fondées sur le passage du droit d'émettre (jeton) dont le Token Ring est l'implémentation la plus connue.

➤ Les méthodes à contention

Les méthodes à contention ou **CSMA** (*Carrier Send Multiple Access* ou accès multiple avec écoute de la porteuse) sont utilisées dans deux types de réseaux :

– le réseau AppleTalk (**CSMA/CA**, *Collision Avoidance* ou à prévention de collision). L'architecture réseau d'Apple est essentiellement destinée au partage de l'imprimante LaserWriter, d'un débit très réduit (230,4 kbit/s), cette architecture est, aujourd'hui, obsolète ;

– le réseau dit « Ethernet » ou **CSMA/CD** (*Collision Detection* ou à détection de collision). D'origine DEC, INTEL et XEROX (Ethernet DIX standard ou Ethernet V2), Ethernet utilise une méthode d'accès qui a été normalisée par l'IEEE (802.3) et par l'ISO (8802.3), il représente plus de 90 % des réseaux locaux installés.

© Dunod – La photocopie non autorisée est un délit

➤ Les méthodes à réservation

Dérivées du polling/selecting, les méthodes à réservation en diffèrent par une distribution décentralisée du droit d'émettre. L'autorisation d'émettre est matérialisée par une trame particulière : le jeton ou *token* qui circule d'équipement en équipement soit dans l'ordre physique des éléments (Token Ring ou anneau à jeton) soit dans l'ordre logique des stations (Token bus ou bus à jeton). Le jeton circule en permanence sur le réseau, toutes les stations le reçoivent successivement et ne peuvent émettre des données que s'il est libre.

L'adressage MAC

➤ Généralités

L'adresse MAC désigne de manière unique une station sur le réseau. À des fins de facilité d'administration, elle est gravée dans l'adaptateur réseau (**NIC**, *Network Interface Card*) par le fabriquant. Pour garantir l'unicité d'adresse, c'est l'IEEE qui les attribue. L'IEEE propose deux formats d'adresse : un format long sur 48 bits et un format court sur 16 bits. La figure 12.15 présente l'adressage IEEE[4], les bits sont représentés dans l'ordre d'émission sur le support (bits de poids faibles devant).

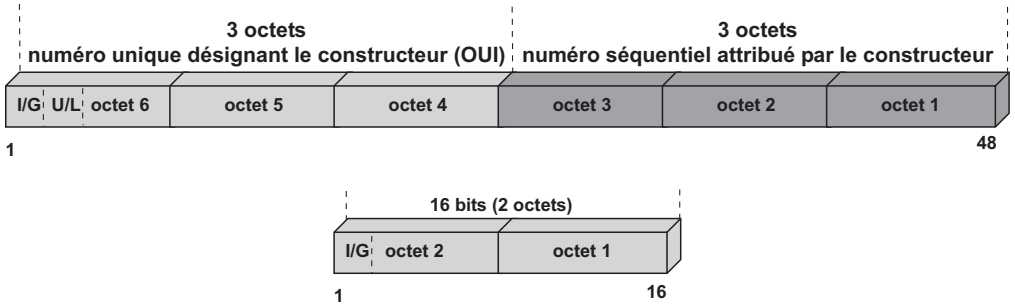


Figure 12.15 Adressage IEEE.

Seul, en principe, l'adressage long est utilisé. Le premier bit (bit I/G) distingue une adresse individuelle ou unicast (I = 0) d'un adressage de groupe (multicast ou broadcast, I = 1). Le bit suivant (bit U/L) détermine si l'adresse qui suit est universelle : adressage IEEE (U = 0) ou local (U = 1). Dans ce dernier cas, c'est à l'administrateur de réseau de gérer l'espace d'adressage et de garantir l'unicité d'adressage. L'adressage IEEE est un adressage à plat, il désigne une machine mais ne permet pas d'en déterminer la position géographique.

Dans l'adressage universel, les 22 bits suivants désignent le constructeur ou le revendeur de l'adaptateur réseau. IEEE attribue à chaque constructeur[5] un ou plusieurs numéros qui l'identifient (**OUI**, *Organization Unit Identifier*). Les 24 bits suivants appartiennent à une série séquentielle et sont inscrits dans l'adaptateur sous la responsabilité du fabricant (**SN**, *Serial Number*). La RFC 1340 récapitule la liste des numéros attribués, un extrait est donné figure 12.16.

4. Devant la multiplication des équipements à identifier, en 1995, l'IEEE a défini un nouveau format d'adressage sur 64 bits (EUI-64).

5. La fourniture par l'IEEE d'un OUI est une prestation payante, le coût actuel est de 1000$ US.

Numéro constructeur (en hexadécimal)	Constructeur	Numéro constructeur (en hexadécimal)	Constructeur
00-00-0C	Cisco	08-00-02	3Com-Bridge
00-00-0F	NexT	08-00-05	Symbolics
00-00-10	Sytek	08-00-06	Siemens Nixdorf
00-00-1D	Cabletron	08-00-07	Apple
00-00-2A	TRW	08-00-09	HP
00-00-5E	IANA	08-00-0A	Nestar Systems
00-00-65	Network General	08-00-0B	Unisys
00-00-6B	MIPS	08-00-10	AT & T
00-00-77	MIPS	08-00-11	Tektronics
00-00-81	Synoptics	08-00-14	Excelan
00-00-89	Cayman Systems	08-00-20	Sun
00-00-93	Proteon	08-00-2B	DEC
00-00-A2	Wellfleet	08-00-38	Bull
00-00-A7	NCD	08-00-39	Spider
00-00-A9	Network Systems	08-00-46	Sony
00-00-AA	Xerox	08-00-4E	BICC
00-00-C0	Western Digital	08-00-5A	IBM
00-00-C9	Emulex	08-00-69	Silicon Graphics
00-AA-00	Intel	08-00-6E	Excelan
00-DD-00	Ungermann-Bass	08-00-7C	Vitalink
00-DD-01	Ungermann-Bass	08-00-90	Retix

Figure 12.16 Extrait de la RFC 1340.

➤ Les différentes adresses MAC

L'adresse individuelle ou unicast

L'adresse unicast est utilisée pour les échanges entre stations. Notons que tout adaptateur possède une adresse unicast gravée lors de sa fabrication, mais il est aussi susceptible de se voir attribuer par l'administrateur une adresse d'unicast locale (bit L à 1). Pour des raisons d'identification de la composante locale, cette facilité est surtout employée dans les réseaux en anneau à jeton.

L'adresse de diffusion généralisée ou broadcast

Une adresse de broadcast est une adresse de diffusion générale. Tous les bits sont à 1 (FF-FF-FF-FF-FF-FF). Cette adresse est notamment utilisée pour chercher une station dont on connaît l'adresse IP mais pas l'adresse MAC (protocole de résolution d'adresses, ARP ou *Address Resolution Protocol*). Seule, la station intéressée répond en fournissant son adresse MAC. Lors de cet échange de messages, les deux stations ont établi des tables de correspondance entre l'adresse IP de la station et son adresse MAC. Ensuite, seule cette adresse MAC sera utilisée pour les échanges suivants.

L'usage abusif de broadcast peut être très pénalisant, surtout sur des liens WAN généralement à débit faible. Le comportement des systèmes d'interconnexion face aux broadcast diffèrent. Les routeurs ne diffusent pas les broadcasts. Les ponts les diffusent, mais il est possible de les paramétrer pour en interdire la transmission.

© Dunod – La photocopie non autorisée est un délit

L'adresse de diffusion restreinte ou multicast

Une adresse de multicast ou de groupe (bit G = 1) désigne un ensemble de stations. Les applications fournissent à la station (couche MAC) la liste des adresses de groupe auxquelles elle doit répondre (abonnement). Ces adresses sont utilisées, par exemple, pour la diffusion vidéo. Des plages d'adresses multicasts ont été définies pour permettre l'encapsulation d'adresses IP multicast, cette plage s'étend de :

01-00-5E-00-00-00 à 01-00-5E-7F-FF-FF (RFC 1112)

La figure 12.17 montre comment est réalisée la construction d'une adresse multicast IEEE (adresse MAC) à partir d'une adresse IP multicast (classe D).

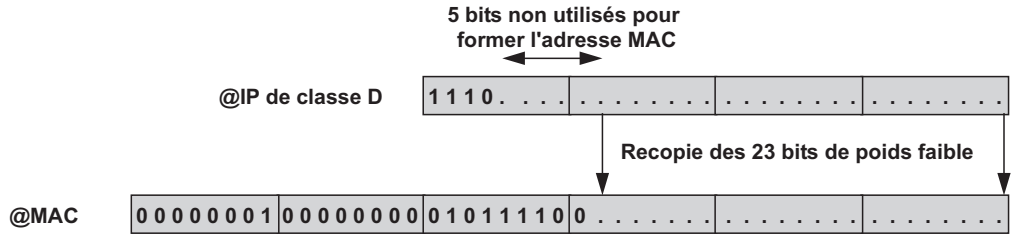

5 bits non utilisés pour former l'adresse MAC
@IP de classe D
1 1 1 0 . . . .
Recopie des 23 bits de poids faible
@MAC
0 0 0 0 0 0 0 1
0 0 0 0 0 0 0 0
0 1 0 1 1 1 1 0
0 . . . . . .

Figure 12.17 Construction d'une @MAC multicast à partir d'une @IP de classe D.

➤ Format canonique et non canonique.

Les bits d'adresse sont toujours transmis bits de poids faible en premier (figure 12.15), ce qui ne correspond pas à l'écriture naturelle des valeurs. Lorsque l'adresse est écrite au format IEEE (bit de poids faible en tête, octet de poids fort devant) l'adresse est dite au format canonique, les valeurs des différents octets s'écrivent en les séparant par « : », dans le cas inverse (écriture naturelle), le format est dit non canonique et les différents octets sont écrits en les séparant par un tiret (figure 12.16). Les réseaux de type Ethernet utilisent le format canonique, les réseaux Token Ring le format non canonique.

Le contrôle d'erreur

L'en-queue contient le champ de contrôle d'erreur par CRC[6] sur 32 bits (**FCS**, *Frame Control Sequence*). Le polynôme générateur, identique pour tous les types de réseaux normalisés par IEEE, est :

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + 1$$

La couche MAC rejette toute trame erronée mais n'effectue aucune reprise sur erreur. Cette tâche sera éventuellement réalisée par les couches supérieures. La figure 12.18 représente le format général de la trame MAC. L'en-tête et l'en-queue sont spécifiques à chaque type de réseau.

6. Voir section 6.2.1 pour le mode de calcul du CRC ou FCS.

Figure 12.18 Format général de la trame MAC.

12.2.3 La couche liaison (LLC)

Généralités

La sous-couche **LLC** (*Logical Link Control*) assure un service comparable à celui offert par la couche liaison du modèle de référence. Elle masque à la couche supérieure le type de réseau utilisé (Ethernet, Token Ring...). Les services de la sous-couche LLC sont accessibles à partir d'un point d'accès **LSAP** (*Link Service Access Point* ou point d'accès au service de liaison). Pour distinguer les deux extrémités de la relation, ces points sont respectivement appelés **DSAP** pour la machine destination (*Destination Service Access Point*) et **SSAP** pour la machine source (*Source Service Access Point*). La figure 12.19 illustre ces notions.

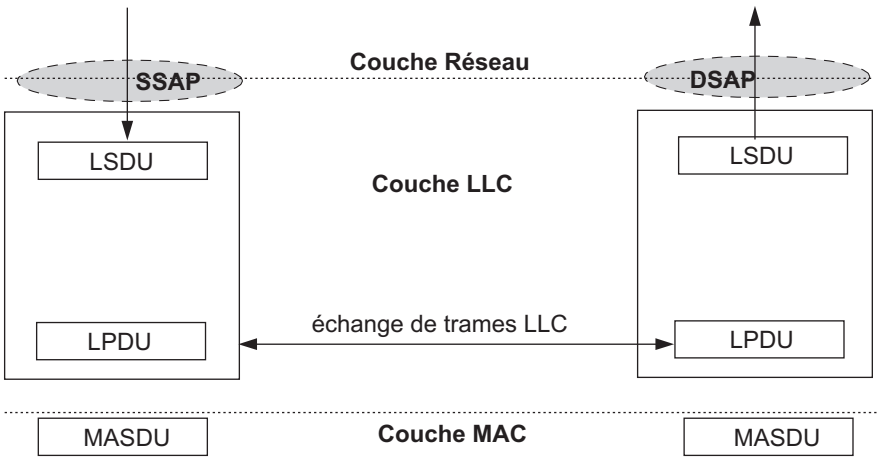


Figure 12.19 Notions de point d'accès selon le modèle OSI.

Les unités de données délivrées par ou à la couche supérieure forment des **LSDU** (*Link Service Data Unit*), celles-ci transmettent à la couche liaison les informations nécessaires à l'envoi des données (adresses MAC source et destination, niveau de priorité, données...). Les sous-couches LLC s'échangent des **LPDU** (*Link Protocol Data Unit*) dont le format est similaire à celui des trames d'HDLC (figure 12.20).

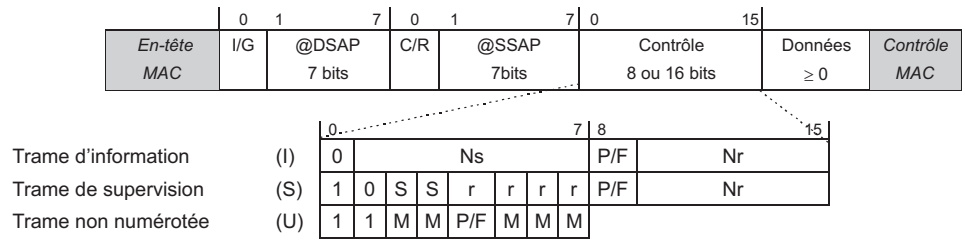

0 1 7 0 1 7 0 15
En-tête MAC
I/G
@DSAP 7 bits
C/R
@SSAP 7bits
Contrôle 8 ou 16 bits
Données ≥ 0
Contrôle MAC
0 7 8 15
Trame d'information (I) 0 Ns P/F Nr
Trame de supervision (S) 1 0 S S r r r r P/F Nr
Trame non numérotée (U) 1 1 M M P/F M M M

Figure 12.20 Format général des trames LLC.

© Dunod – La photocopie non autorisée est un délit

Les adresses DSAP et SSAP sont codées sur 7 bits (128 points d'accès). La notion d'adresse LSAP autorise la cohabitation de protocoles différents pour une même carte adaptateur (adresse MAC). Certaines valeurs sont réservées, le tableau de la figure 12.21 fournit quelques exemples d'adresses LSAP.

LSAP	Service identifié
0X'00'	Null SAP
0X'02'	LLC Management
0X'06'	Internet ARPA
0X'AA'	SNAP
0X'F0'	NETBIOS
0X'FE'	ISO

Figure 12.21 Exemples d'adresses LSAP.

Le bit I/G indique s'il s'agit d'un DSAP individuel (I = 0) ou de groupe (I = 1). Tous les bits du champ adresse à 1 correspondent à l'adresse de diffusion générale (broadcast).

Le bit C/R distingue une trame de commande (C/R = 0) ou de réponse (C/R = 1), identifiant ainsi l'initiateur des échanges, il a une fonction identique au champ adresse de LAP-B, il sert à distinguer le bit P du bit F (commande ou Poll C/R = 0 et P = 1, réponse C/R = 1 et F = 1).

À l'instar d'HDLC, le champ contrôle, sur 8 ou 16 bits, identifie le type de trame (I, S, U), les trames I et S contiennent les compteurs Ns (compteur de trames émises) et Nr (compteur de trames reçues) sur 3 bits (champ de 8 bits, numérotation des trames modulo 8) ou 7 bits (champ contrôle sur 16 bits, numérotation des trames modulo 128). Les bits r sont réservés pour un usage ultérieur.

La couche LLC offre, selon les besoins, trois types de services : LLC1, LLC2 et LLC3.

Les services de la couche LLC

➤ Le service LLC de type 1

Le service LLC1 est un service en mode datagramme. Il n'y a, par conséquent, ni acquittement, ni contrôle de séquencement, ni contrôle de flux et de reprise sur erreur. Le contrôle d'erreur est réalisé par la couche MAC qui rejette toute trame erronée. C'est le service le plus simple et pratiquement le seul utilisé dans les réseaux locaux. Le service rendu à la couche supérieure est limité, c'est à celle-ci de prendre en compte les lacunes du service LLC1. Généralement, dans les réseaux locaux, c'est la couche transport qui assure ce rôle. LLC1 ne met en œuvre que deux primitives :

– L_Data. request (@Source, @Destination, LSDU, Priorité) ;

– L_Data.indication (@Source, @Destination, LSDU, Priorité).

Les adresses source (@Source) et destination (@Destination) sont constituées de l'association du LSAP source ou destination et de l'adresse MAC source ou destination. Ces valeurs sont nécessaires pour construire la trame MAC. Le champ priorité n'est exploité que si la sous-couche MAC offre ce service.

LLC1 utilise la trame de type UI (*Unumbered Information*, champ de contrôle à 0x03) représentée figure 12.22.

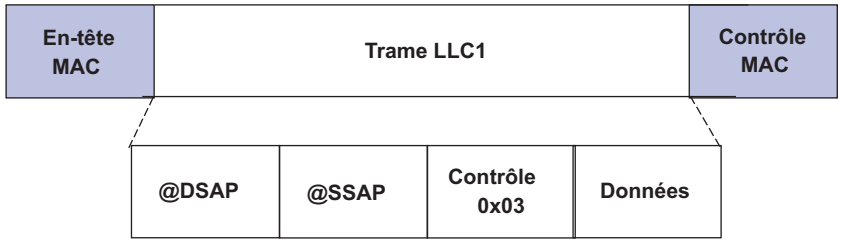


Figure 12.22 Format de la trame LLC1.

➤ Le service LLC de type 2

Le service LLC2 est un service en mode connecté similaire à HDLC (LAP-B). Il assure l'acquittement, le contrôle de flux, le contrôle de séquencement et la reprise sur erreur. Une connexion est identifiée par l'association de l'adresse LSAP et de l'adresse MAC de la station (figure 12.23).

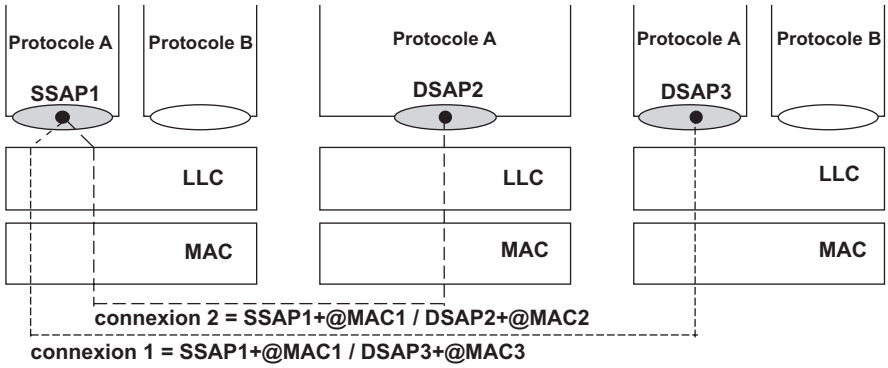


Figure 12.23 Mode connecté de LLC2.

LLC2 est un service en mode connecté, un échange de données ne peut avoir lieu qu'au sein d'une connexion et, par conséquent, ce mode interdit la diffusion.

➤ Le service LLC de type 3

Intermédiaire entre le service LLC1, simple mais non sécurisé, et le service LLC2 complexe mais qui certifie la délivrance des données, LLC3 implémente un service sans connexion (simplicité) mais avec acquittement (sécurisation des échanges) ; c'est un service de datagrammes acquittés. Si l'acquittement n'est pas arrivé à l'échéance du temporisateur, il n'y a pas de reprise, la perte est signalée aux couches supérieures. Ce sont elles qui décideront de l'éventuelle réémission de la même trame ou d'une trame contenant les nouvelles valeurs du processus en cours.

Destiné aux systèmes temps réel (processus industriel), ce service, par sa simplicité, autorise son implémentation sur des systèmes simples (capteurs...). Le protocole prévoit un mécanisme de polling, le capteur n'envoie des données que lorsqu'il y est invité, ce qui limite les mécanismes à implémenter dans celui-ci.

© Dunod – La photocopie non autorisée est un délit

La sous-couche SNAP (SubNetwork Access Protocol)

L'encapsulation LLC présente deux inconvénients : d'une part, elle n'identifie pas tous les protocoles notamment le protocole ARP (*Address Resolution Protocol*) de la pile TCP/IP et d'autre part, en introduisant un en-tête de 3 octets, elle détruit l'alignement de la trame sur des mots machines grévant ainsi les performances. D'où la définition d'une encapsulation supplémentaire réalisée par une sous-couche spécifique : la sous-couche **SNAP** (*SubNetwork Access Protocol*) qui introduit un champ d'identification supplémentaire **PIH** (*Protocol Identifier Header*). La figure 12.24 représente l'encapsulation SNAP pour une trame MAC IEEE 802.3. Les différents champs de la trame IEEE 802.3 seront expliqués lors de l'étude de ce type de réseau. Dans ce mode d'encapsulation, les champs DSAP et SSAP de la trame LLC sont à 0xAA, ils identifient l'encapsulation SNAP.

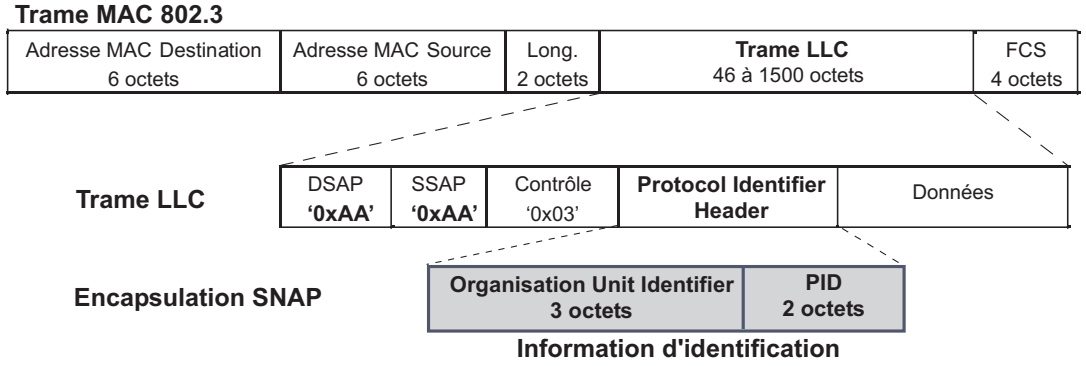


Figure 12.24 L'encapsulation SNAP.

Le **PIH** (*Protocol Identifier Header*) est divisé en deux champs : le champ **OUI** (*Organization Unit Identifier*) et le champ **PID** (*Protocol Identifier*). La valeur « 0 » du champ OUI indique que le champ PID est codé de la même façon que le champ Ethertype de la trame Ethernet.

L'encapsulation SNAP est essentiellement utilisée dans l'environnement Token Ring et dans les modes d'encapsulation utilisés par les protocoles haut débit (Frame Relay, RFC 1490 et ATM, RFC 1483).

Les interfaces de programmation NDIS et ODI

Afin d'éviter d'avoir à développer des piles protocolaires spécifiques à telle ou telle carte, les fabricants de cartes réseaux (**NIC**, *Network Interface Card*) et les éditeurs de logiciels ont introduit, entre les couches logicielles et la carte transporteur, une couche d'abstraction. Cette couche, **NDIS** pour *Network Data Interface Specification* d'origine Microsoft et 3COM ou **ODI** pour *Open Data link Interface* de Novell n'est pas une couche au sens OSI du terme puisqu'elle ne rend aucun service. Elle masque aux couches supérieures les différentes implémentations des cartes.

Outre l'indépendance des piles vis-à-vis des cartes, NDIS et ODI autorisent le chargement et l'utilisation simultanée de plusieurs protocoles réseaux sur une même interface physique.

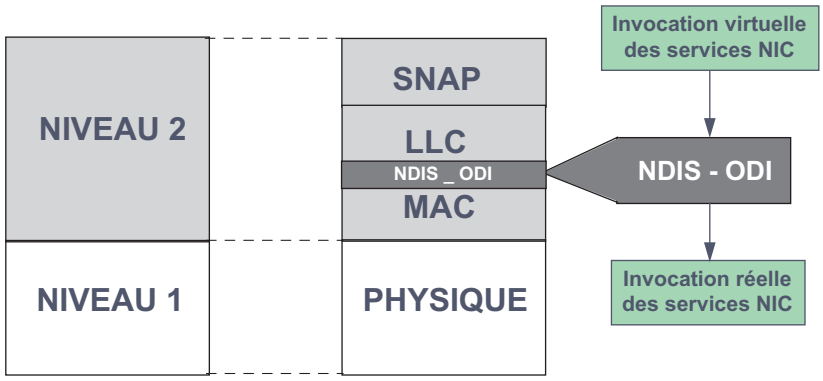


Figure 12.25 Les interfaces de programmation.

12.3 LES RÉSEAUX CSMA/CD, IEEE 802.3/ETHERNET

12.3.1 Les origines d'Ethernet

Les protocoles à contention ont pour origine la méthode d'accès radio Aloha du réseau radio de l'université d'Hawaï (1970). Une station qui avait un message à transmettre l'émettait sans se préoccuper des autres stations. Si le message était pollué par une autre émission (collision), il était retransmis. Cette méthode est d'autant moins efficace que le nombre de stations augmente. Cependant, elle est très simple à implémenter. La méthode dite **CSMA/CD** (*Carrier Sense Multiple Access, Collision Detection*) dérive de cette approche. D'abord baptisé Alto Aloha, l'Ethernet[7] (réseau dans l'Ether) est développé chez Xerox par Robert Metcalfe dans les laboratoires d'Alto (Alto Aloha Network) en 1973. Cette première version sur câble coaxial offrait un débit de 3 Mbit/s. Associant Digital, Intel et Xerox (**DIX**), Bob Metcalfe fit évoluer sa version vers 10 Mbit/s (Ethernet DIX, 1980). Les spécifications définitives (Ethernet V2, 1982) ont été reprises par l'IEEE pour donner naissance aux spécifications IEEE 802.3 10 Base 5 (1985), puis par l'ISO (IS 8802.3) en 1989. Aujourd'hui cette technique domine largement le marché, et fait un retour aux sources avec le développement de la norme 802.11 (réseaux sans fil).

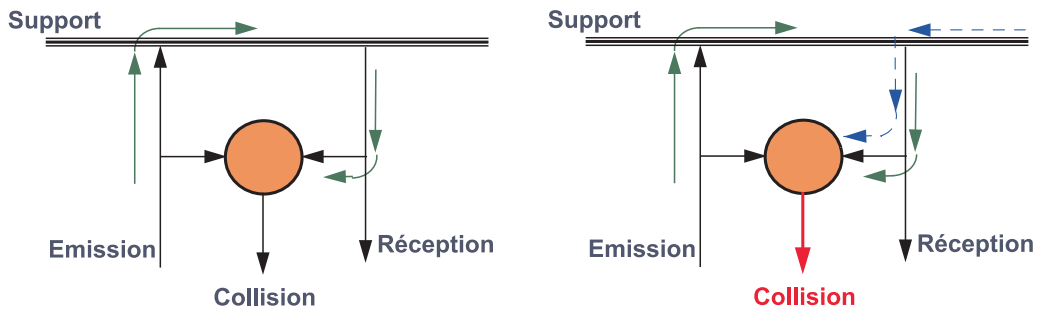
12.3.2 Principe du CSMA/CD

Le principe de base du CSMA/CD repose sur la diffusion des messages à toutes les stations (réseau à diffusion). Lorsqu'une station désire émettre, elle écoute le réseau, si aucun message n'est en cours de diffusion (silence) elle émet, sinon, elle diffère son émission jusqu'à ce que le support soit libre (attente active).

Cette méthode ne peut garantir que deux stations ne décèleront pas le silence en même temps et émettront simultanément leur message. Chaque message est pollué par l'autre (collision) et devient inexploitable. Il est, alors, inutile de continuer à émettre un message incompréhensible. Aussi, lorsqu'une station détecte une collision, elle cesse ses émissions.

7. Ethernet est une marque déposée par Xerox. Ce nom est passé dans le langage commun, mais s'écrit toujours avec une majuscule.

© Dunod – La photocopie non autorisée est un délit



Le signal reçu est identique au signal émis, il n'y a pas de collision

Le signal reçu diffère du signal émis, il y a collision

Figure 12.26 Principe de la détection de collision.

Pour détecter les collisions (figure 12.26), chaque station écoute le support durant son émission. Si elle décèle une perturbation de son message (les niveaux électriques sur le support ne correspondent pas à son émission), elle arrête son émission et arme un temporisateur (aléatoire, algorithme dit BEB, voir section 12.3.3). À l'échéance du temporisateur la station écoute le support, s'il est libre, elle retransmet le message tout en surveillant son émission (détection de collision). C'est la couche MAC qui réalise la reprise sur collision, ceci évite de remonter dans les couches hautes et de pénaliser les performances du réseau. La figure 12.27 illustre ce mécanisme.

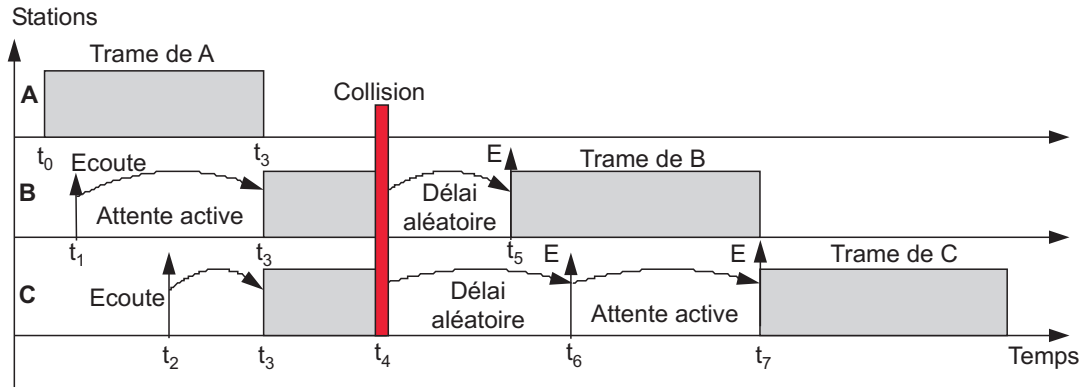


Figure 12.27 Principe du CSMA/CD.

La station **A** diffuse son message (t_0 à t_3). La station **B**, avant d'émettre, se met à l'écoute (t_1). Le support est occupé, elle diffère son émission, mais reste à l'écoute (attente active). De même **C**, en t_2, se porte à l'écoute et retarde son émission. En t_3, **A** cesse d'émettre, **B** et **C** détectent le silence, ils émettent simultanément. En t_4, chacune des stations détecte que son message est altéré, la collision est détectée. **B** et **C** cessent leur émission et déclenchent une temporisation aléatoire. En t_5, le timer de **B** arrive à échéance. Le canal étant libre, **B** émet. En t_6, **C** détecte le support occupé et diffère son émission jusqu'au temps t_7.

12.3.3 Caractéristiques communes aux réseaux Ethernet/802.3

Fenêtre de collision

La fenêtre de collision correspond au temps minimal pendant lequel une station doit émettre pour détecter la collision la plus tardive que son message est susceptible de subir. Considérons (figure 12.28) les deux stations les plus éloignées du réseau : **A** et **B**. En 1, **A** émet, tant que le message de **A** n'est pas parvenu à **B**, cette dernière suppose le support libre (2). **B** émet alors un message juste au moment où le premier bit du message de **A** lui parvient (3). La station **B** détecte instantanément la collision et cesse son émission (3). Pour que **A** puisse détecter que son message a subi une collision, il est nécessaire que le petit message de **B** lui parvienne et qu'il soit encore en émission à cet instant (4). Ce temps minimal d'émission s'appelle fenêtre de collision, *time slot* ou encore tranche canal. C'est aussi la période de vulnérabilité d'un message.

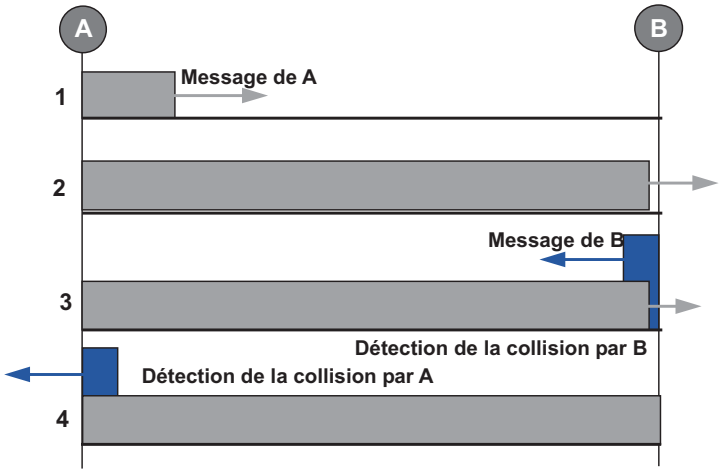


Figure 12.28 Fenêtre de collision.

Ce temps minimal d'émission correspond à 2 fois le temps de propagation d'une trame sur la plus grande distance du réseau (2 500 m), traversée des répéteurs ou autres organes d'interconnexion des brins compris. Fixé à 51,2 μs, ce temps correspond, pour un débit de 10 Mbit/s, à l'émission de 512 bits, soit 64 octets. Cette exigence implique, en cas de message de longueur inférieure, qu'une séquence de bourrage (*padding*) soit insérée derrière les données utiles. Un pointeur de longueur permet au récepteur d'extraire les données. La figure 12.29 illustre la structure générale de la trame 802.3.

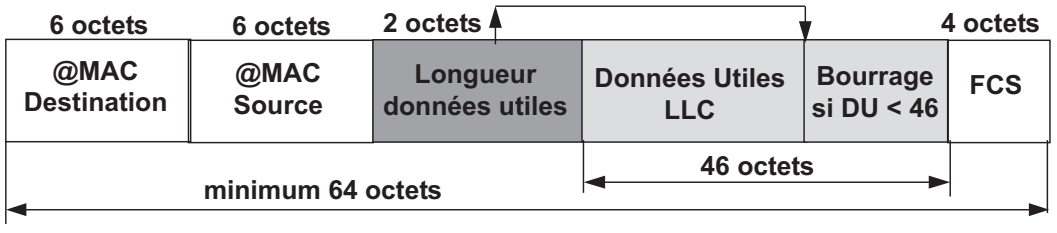


Figure 12.29 Structure générale d'une trame 802.3.

© Dunod – La photocopie non autorisée est un délit

Le champ longueur des données utiles, sur deux octets, différentie les spécifications Ethernet V2 et IEEE 802.3, en conséquence, les deux réseaux sont incompatibles. Dans la version Ethernet V2, ce champ identifie le protocole supérieur, c'est à ce dernier que revient la tâche d'extraire les données utiles du champ données.

Dans l'exemple de la figure 12.28, la station **B** a cessé son émission immédiatement après avoir détecté la collision, son message est donc très court. Pour être certain qu'un message minimal arrive à **A** et que celui-ci détecte bien la collision, **B** émet une séquence de brouillage de 32 bits à 1 (3,2 μs) appelée *jam interval*.

Les évolutions récentes d'Ethernet vers des débits plus élevés ont posé le problème du maintien de cette fenêtre à 51,2 μs. Par exemple, à 100 Mbit/s, la trame minimale devient de 640 octets, c'est-à-dire que compte tenu des données de bourrage l'augmentation du débit vu des applications serait quasiment nulle pour les petits messages. Dans ces conditions et pour assurer la compatibilité entre les différentes versions, la trame minimale de 64 octets a été maintenue. Si le débit croît, la fenêtre de collision décroît dans les mêmes proportions, et par conséquent la distance maximale entre deux stations aussi (diamètre du réseau). Le tableau de la figure 12.30 illustre cette relation.

Débit	Fenêtre de collision	Diamètre du réseau
10 Mbit/s	51,2 μs	2 500 m
100 Mbit/s	5,12 μs	250 m
1 000 Mbit/s	0,512 μs	25 m

Figure 12.30 Relation débit et diamètre du réseau.

Algorithme du BEB

Le **BEB** (*Binary Exponentiel Backoff*) ou encore algorithme de ralentissement exponentiel, détermine le délai aléatoire d'attente avant que la station ne réessaie, après collision, une émission (figure 12.31). Après une collision, une station ne peut émettre qu'après un délai défini par :

$$T = K \cdot TimeSlot$$

K est un nombre aléatoire entier généré par l'émetteur et compris dans l'intervalle :

$$K = \left[0, 2^n - 1\right] \text{ avec } n \leqslant 10$$

où n représente le nombre de collisions successives détectées par la station pour l'émission d'un même message. Après 16 tentatives, l'émetteur abandonne l'émission.

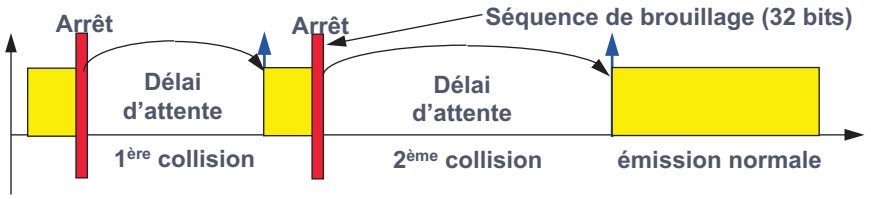


Figure 12.31 Principe du BEB.

Remarquons :

– que si deux stations entrent en collision, la probabilité pour qu'elles en subissent une seconde est de 0,5 (tirage de 0 ou 1) ;

– qu'il est, dans ces conditions, impossible de borner le temps d'attente avant l'émission d'un message. Le CSMA/CD est une méthode d'accès probabiliste et non déterministe. Ce protocole ne convient pas au temps réel, ni aux transferts isochrones (voix, vidéo).

Le silence intermessage (IFG, InterFrame Gap)

L'IFG correspond au temps minimal entre deux messages. Une station (à 10 Mbit/s) avant d'émettre doit détecter un silence d'au moins 9,6 µs. Ce temps permet :

– d'une part, à l'électronique de bien discerner deux messages ;

– et, d'autre part, l'absorption d'éventuelles réflexions pour éviter la détection de collisions fantômes.

12.3.4 Trame Ethernet/IEEE 802.3

La trame IEEE 802.3 est représentée en figure 12.32. Le codage est du type Manchester. Un préambule de 7 octets permet la synchronisation bit. La synchronisation caractère est assurée par le fanion de début de trame (**SFD**, *Start Frame Delimitor*), les deux bits à 1 marque le début de la trame. Les champs adresses contiennent les adresses MAC destination et source. Un pointeur, sur 2 octets, indique la longueur utile du champ données. Le champ données est suivi d'un contrôle d'erreur de type CRC : le FCS sur 4 octets.

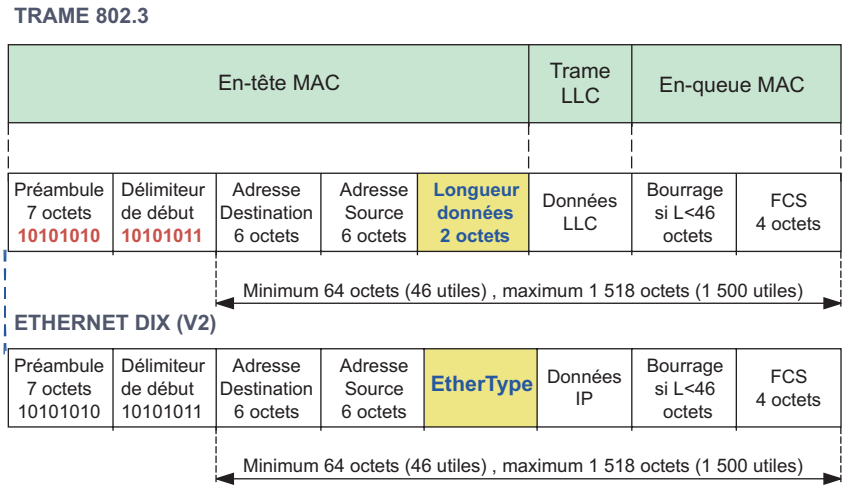

TRAME 802.3
En-tête MAC
Trame LLC
En-queue MAC
Préambule 7 octets 10101010
Délimiteur de début 10101011
Adresse Destination 6 octets
Adresse Source 6 octets
Longueur données 2 octets
Données LLC
Bourrage si L<46 octets
FCS 4 octets
Minimum 64 octets (46 utiles) , maximum 1 518 octets (1 500 utiles)
ETHERNET DIX (V2)
Préambule 7 octets 10101010
Délimiteur de début 10101011
Adresse Destination 6 octets
Adresse Source 6 octets
EtherType
Données IP
Bourrage si L<46 octets
FCS 4 octets
Minimum 64 octets (46 utiles) , maximum 1 518 octets (1 500 utiles)

Figure 12.32 Format de la trame Ethernet/IEEE 802.3.

La trame Ethernet DIX (Dec, Intel, Xerox) diffère de la trame IEEE 802.3, par le champ longueur de données. Celui-ci est remplacé par l'identifiant, sur deux octets, du protocole supérieur (Ethertype). C'est à ce dernier de gérer la longueur des données utiles. Par exemple, le protocole IP de TCP/IP est identifié par la valeur 2 048 (0x0800).

© Dunod – La photocopie non autorisée est un délit

12.3.5 Les différentes versions d'Ethernet

Ethernet épais, IEEE 802.3 10 base 5

Les appellations IEEE désignent d'abord le sous-comité (802.3), le type de modulation (bande de base ou large bande : *broad band*) et le diamètre du réseau. La version 10 Base 5, (10 Mbit/s en bande de base sur câble coaxial d'une longueur maximale par segment de 500 m) utilise un codage Manchester. La figure 12.33 représente cette version d'origine de l'Ethernet.

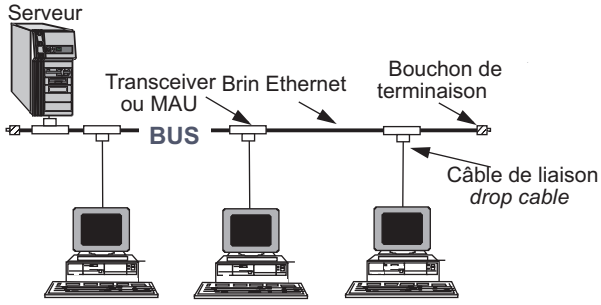


Figure 12.33 Le réseau Ethernet Jaune.

Chaque station est équipée d'une interface « Ethernet » (**NIC**, *Network Interface Card*) généralement appelée carte transporteur ou carte « Ethernet ». Cet équipement assure l'adaptation physique (niveaux électriques, encodage...) et gère l'algorithme CSMA/CD. Dans la version 10 base 5, un connecteur DB15 (Cannon 15 broches) permet le raccordement du câble de liaison (*Drop cable*) au *transceiver* ou **MAU** (*Medium Attachment Unit* ou unité d'attachement au support). Le MAU contient l'électronique d'émission et de réception, il assure la détection des collisions qu'il signale à la station (figure 12.26). Le *transceiver* se raccorde au coaxial par un système dit de prise vampire (le raccordement d'une nouvelle station se fait sans interrompre le trafic).

Le *drop cable*, d'une longueur maximale de 50 m, est constitué de paires torsadées (5 paires). Le câble coaxial est un câble épais de couleur jaune (Ethernet jaune) dont les principales caractéristiques sont : diamètre un demi-pouce, impédance 50 Ω, coefficient de vélocité 0,77. Un *transceiver* peut être connecté tous les 2,5 m avec un maximum de 100 stations actives par segment de 500 m. La longueur totale du réseau peut atteindre 2,5 km (5 segments). Il est recommandé de n'utiliser que des segments dont la longueur est un multiple impair de 23,4 m (longueur d'onde du signal à 10 MHz

Cette version d'Ethernet n'est pratiquement plus utilisée que dans des environnements compromis (rayonnement électromagnétique), lorsque l'on veut garantir la confidentialité des échanges (pas de rayonnement du câble coaxial). Le câblage en bus étant moins volumineux qu'un câblage étoile, cette version trouve encore son utilité à chaque fois que des problèmes d'encombrement se posent.

Ethernet fin, IEEE 802.3 10 base 2

Compte tenu des difficultés de câblage de la version 10 base 5, une version économique a été réalisée avec du câble coaxial fin (Thin Ethernet). Dans cette version, les fonctions du *transceiver* sont remplies par la carte transporteur (MAU intégré à la carte). De ce fait, le bus coaxial est

connecté directement sur la carte par l'intermédiaire d'un T vissé BNC (*Barrel Neck Connector*). La longueur maximale d'un segment est de 185 m et chaque segment peut accueillir un maximum de 30 stations. La figure 12.34 présente cette version du réseau Ethernet.

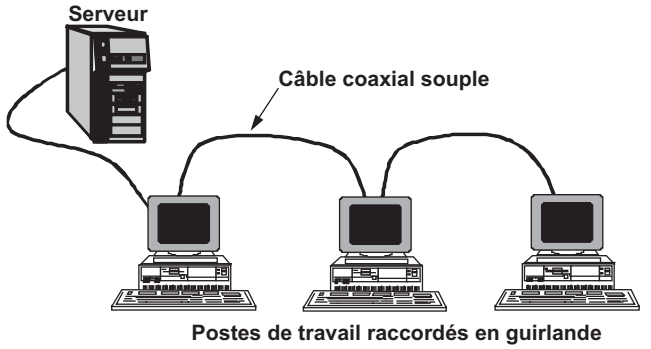


Figure 12.34 L'Ethernet fin.

Cette architecture physique de réseau est recommandée pour la réalisation de petit réseau d'une dizaine de machines, c'est la plus économique.

Ethernet sur paires torsadées, IEEE 802.3 10 base T

➤ Origine

Compte tenu des problèmes en relation avec le câblage, AT&T a imaginé de réutiliser le câblage téléphonique préexistant dans les immeubles de bureaux pour la réalisation de réseau. Le réseau devait alors passer d'une topologie bus à une topologie physique étoile, assurer la diffusion des messages et la détection des collisions. La solution adoptée par AT&T consiste simplement à émuler un bus dans un boîtier : le hub, chargé d'une part de concentrer les connexions et d'autre part d'assurer la diffusion des messages (figure 12.35).

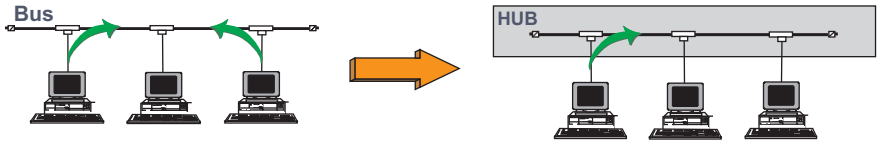


Figure 12.35 Passage du bus à l'étoile.

La liaison hub/station était réalisée en paires torsadées (1 paire émission, 1 paire réception), cela imposait deux contraintes : l'une de débit, l'autre de distance. Ce réseau fonctionnait à 1 Mbit/s, les stations étaient connectées sur des concentrateurs répéteurs (**hub**) et la distance entre le hub et une station était limitée à 250 m. Cette architecture (802.3 1 base 5 ou Starlan), complètement obsolète, est à l'origine de la version à 10 Mbit/s (802.3 10 base T, T pour *Twised pair*) qui en reprend les principes.

➤ Ethernet, 802.3 10 base T

La version 10 base T reprend les principes architecturaux du réseau Starlan, c'est un réseau en étoiles hiérarchisées (figure 12.36). Les hubs assurent :

© Dunod – La photocopie non autorisée est un délit

– les fonctions de diffusion des messages (émulation de bus, deux stations connectées au même hub ne reçoivent le signal de l'autre que via le hub de tête) ;
– la détection des collisions (le hub diffuse un signal de collision vers les autres stations) ;
– la détection de stations bavardes (fonction *Jabber* : message d'une durée supérieure à 150 ms).

En cas de collisions multiples, le hub segmente le réseau. Le débit est de 10 Mbit/s, la longueur d'un brin est limitée à 100 m (distance entre un hub et une station ou entre deux hubs), cette longueur est portée à 150 m si l'atténuation est inférieure à 11,5 dB, le nombre de niveaux est fixé à trois.

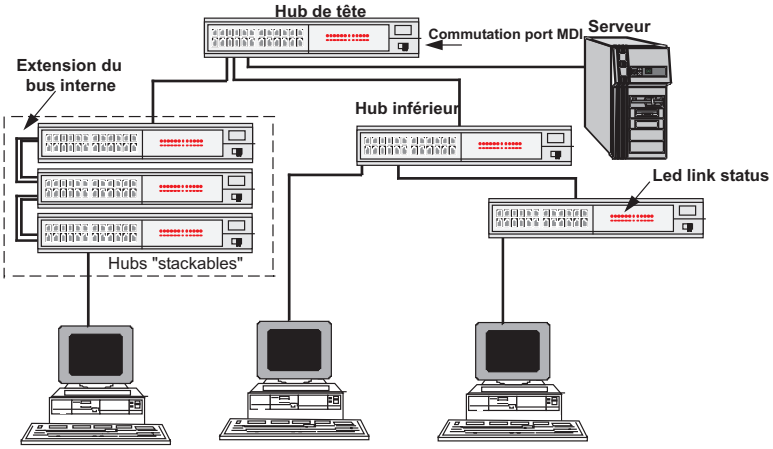


Figure 12.36 Architecture du réseau 10 base T.

Un signal particulier, le *link status* (état de la ligne), permet, par la visualisation de diodes **LED** (*Light Emitting Diode*), de contrôler la continuité du lien entre le hub et la station (*link integrity test function*). En l'absence d'émission, le hub et la carte réseau émettent, toutes les 8 secondes, des impulsions de test de 100 ms (impulsions de test de lien ou **LTP**, *Link Test Pulses*). En l'absence de données (données utilisateur ou signal LTP) ou de réception du signal de remplissage (**TP_IDL**, *Twisted Pair Idle Signal*), le hub et la carte considèrent le lien défectueux, le voyant *link status* est alors positionné à « OFF » et le port du hub est inhibé.

Sur chaque hub, un interrupteur permet la commutation de la fonction d'un des ports (**MDI**, *Medium Dependent Interface*) en port de répétition vers un hub de niveau supérieur (croisement des paires émission et réception). C'est la fenêtre de collision qui limite le nombre de niveaux admissibles (distance maximale). Pour franchir la barrière des trois niveaux et autoriser un plus grand nombre de stations connectées, les hubs peuvent aussi être empilés par l'extension du bus interne (figure 12.36). Ces hubs, dits « stackables », sont vus par le système comme un seul niveau.

Ethernet à 100 Mbit/s

➤ Généralités

Évolution de la version 10 base T, l'Ethernet 100 Mbit/s (ou Fast Ethernet) résulte des travaux du groupe de travail IEEE 802.14. La compatibilité avec la version 10 base T est assurée par

la reprise du protocole CSMA/CD et le maintien des tailles de trames (64 octets au minimum et 1 518 au maximum). De ce fait, la fenêtre de collision ou tranche canal est réduite à 5,12 μs (512 bits) et le silence entre deux trames successives (IFG, *Inter Frame Gap*) ne vaut plus que 0,96 μs (96 bits). La réduction de la fenêtre de collision par un facteur de 10 (de 51,2 μs à 5,12 μs) induit de fortes contraintes sur le temps de propagation du signal et, par conséquent, sur la distance maximale entre les deux stations les plus éloignées du réseau.

➤ Mixité et autonégociation

Pour permettre l'évolution des réseaux en douceur, les concepteurs ont imaginé des hubs dont chacun des ports pouvait indifféremment fonctionner à 10 ou à 100 Mbit/s en fonction de l'équipement qui y était raccordé. Afin de faciliter les tâches d'administration, les ports détectent eux-mêmes le type d'élément qui leur est raccordé (autonégociation). À cet effet, les équipements 100 Mbit/s remplacent le signal de *link status* du 10 base T par un mot de 16 bits (*Link Code Word*) décrivant les caractéristiques de l'équipement. Les cartes réseaux 100 Mbit/s sont dotés des mêmes fonctionnalités. Le port et la carte s'autoconfigurent sur le plus grand dénominateur commun. Ainsi à un hub 100 Mbit/s, il est possible de connecter des équipements 10 ou 100 Mbit/s, de même une carte 100 Mbit/s peut être raccordée à un hub 10 Mbit/s. Dans la pratique, l'autonégociation peut conduire à un fonctionnement perturbé du réseau (dialogue mal compris occasionnant soit le fonctionnement à 10 Mbits, soit le basculement incessant de 10 à 100 Mbit/s), il est souvent préférable de verrouiller l'équipement terminal sur 10 ou 100 Mbit/s selon les équipements utilisés.

Deux types de hubs ont été réalisés (figure 12.37). Les hubs de classe 1, pratiquement les seuls utilisés permettent l'autonégociation donc la mixité. Cependant, plus rapide, car ils n'ont aucune fonction de modification de codage à réaliser, les hubs de classe 2 autorisent un niveau de cascade, le lien inter-hub ne doit pas dépasser 5 m (**IRL**, *Inter Repeater Link*). Ce nombre de niveaux, sans grande influence sur les distances, autorise plus de stations.

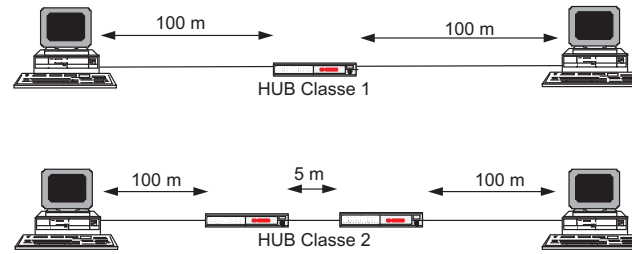


Figure 12.37 Topologie des réseaux 100 base T.

➤ Les différentes implémentations

La norme 100 base T prévoit trois supports différents (figure 12.38). Le 100 base T4 utilise les 4 paires torsadées des câbles de catégorie 3, 4 et 5. Trois paires sont utilisées pour la transmission de données, le quatrième pour gérer la détection de collisions. Les données sont codées 8B/6T (8 bits sur 3 temps d'horloge), ce qui ramène la fréquence d'horloge à 25 MHz (12,5 MHz sur le support).

La version 100 base TX utilise le même câble et les mêmes paires que le 10 base T (UTP catégorie 5). Le codage Manchester est abandonné au profit du codage 4B/5B (16 symboles

© Dunod – La photocopie non autorisée est un délit

parmi 32) ce qui limite la fréquence à 125 MHz sur le support contre 200 si le codage Manchester avait été conservé. Une version sur fibre optique (100 base FX), identique au niveau physique à FDDI, porte la dimension du réseau à 400 m (limite de la fenêtre de collision).

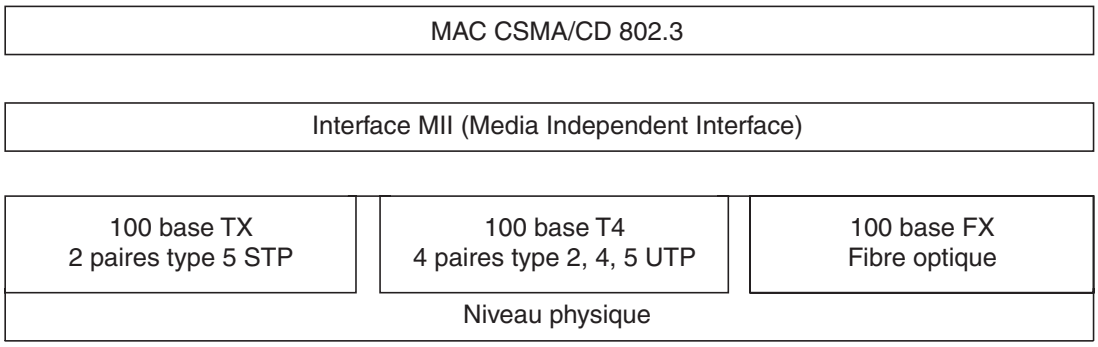


Figure 12.38 Architecture générale de Fast Ethernet.

Le Gigabit Ethernet

Le Gigabit Ethernet est une évolution de l'Ethernet 100 Mbit/s, il fonctionne en diffusion (hub répéteur) mais aussi en commuté. La commutation, étudiée à la section 12.7, est une technique de mise en relation du type point à point. Le commutateur ne diffuse pas la trame, il la réémet sur le seul port où est raccordé le destinataire. Le Gigabit s'est surtout développé dans les environnements commutés, simulant des liaisons point à point, la commutation autorise l'invalidation de la fonction de détection de collision et permet le *full duplex* (émission et réception simultanées). L'architecture générale du Gigabit est représentée figure 12.39.

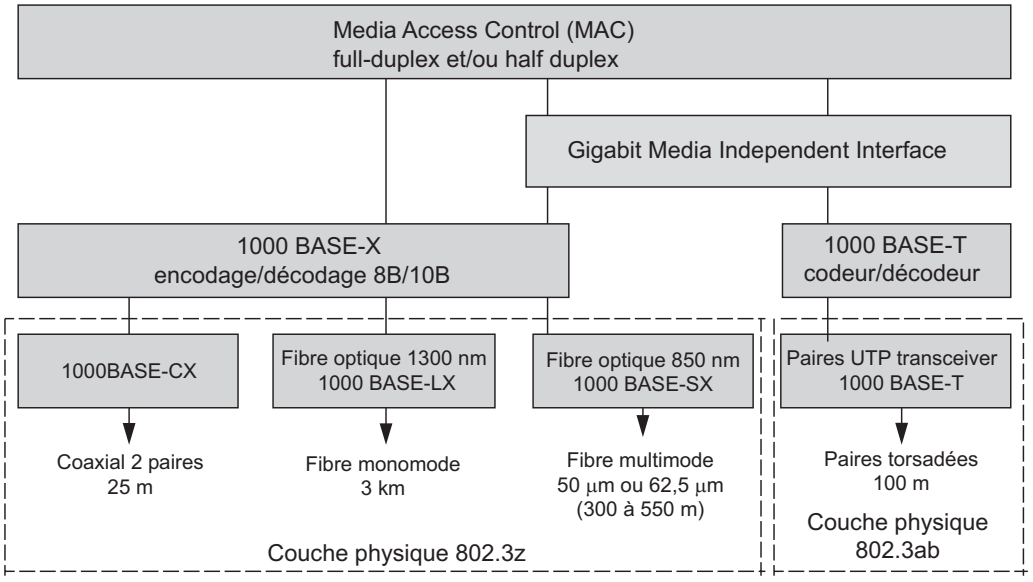


Figure 12.39 Architecture du Gigabit Ethernet

Le Gigabit Ethernet fonctionne en full duplex dans le mode *switch-to-switch* (de commutateur à commutateur), dans le mode *switch-to-end-station* (commutateur à station terminale) et en *half-duplex* pour les stations raccordées directement à un répéteur Ethernet Gigabit (hub).

En mode *half-duplex*, afin de maintenir un diamètre du réseau suffisant (200 m sur paires torsadées) le *time slot* (fenêtre de collision) a été modifié, la trame minimale est portée à 512 octets. En mode *full duplex* (pas de détection de collision), la taille de la trame minimale reste à 512 bits (64 octets), l'IFG (*Inter Frame Gap* ou silence intertrames) à 96 bits.

Une taille minimale de trame de 512 octets conduit à un bourrage important (*carrier extension*) lors du transfert de petits volumes d'information, et donc à un gaspillage de la bande passante. Pour y remédier, le Gigabit implémente une fonction de groupage de trames (*frame bursting*). L'émission de rafales de trames est limitée par un paramètre configurable par l'administrateur (*burst time*) donc la valeur maximale autorise l'émission de 8 ko.

Les équipements Gigabit Ethernet combinent généralement des ports 10, 100 et une ou plusieurs connexions sur fibre optique à 1 000 Mbit/s. La figure 12.40 propose un exemple d'application du Gigabit Ethernet en tant que réseau fédérateur de réseaux à 100 ou 10 Mbit/s. Le commutateur est utilisé en tant que *backbone* (*LAN in a box* ou *collapsed backbone*). Le *backbone* est reporté sur le fond de panier du commutateur, qui remplit alors le rôle de multiplexage des connexions LAN.

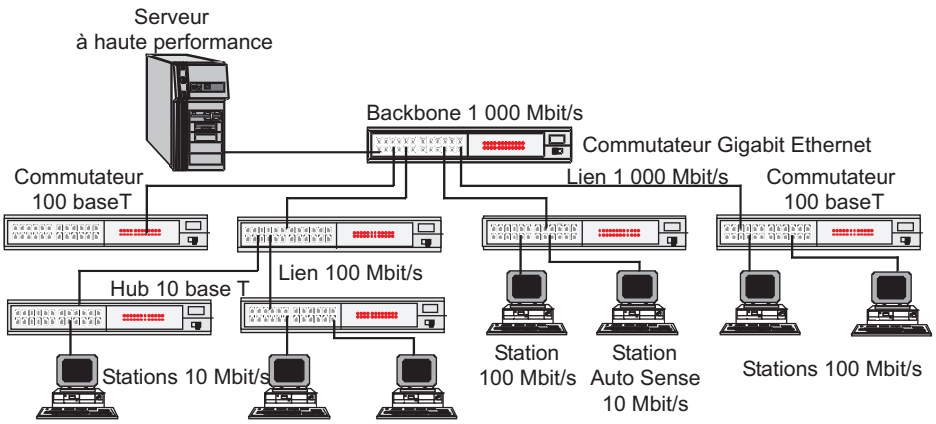


Figure 12.40 Exemple d'utilisation du Gigabit Ethernet.

12.4 L'ANNEAU À JETON, IEEE 802.5

12.4.1 Généralités

La norme IEEE 802.5 (ISO 8802.5) spécifie un réseau local en boucle (figure 12.41) : chaque station est reliée à sa suivante et à sa précédente par un support unidirectionnel. Ce réseau est connu sous le nom de Token Ring[8].

8. Aujourd'hui, largement supplanté par Ethernet, 802.5 reste cependant très présent dans l'environnement IBM. C'est ce qui justifie le maintien d'une étude approfondie dans ce chapitre.

© Dunod – La photocopie non autorisée est un délit

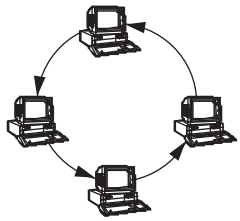


Figure 12.41 Principe de l'anneau.

Publiée en 1985, la norme IEEE 802.5 fut implémentée par IBM dès 1986. IBM est resté le principal acteur du monde Token Ring. L'implémentation d'IBM diffère quelque peu de la norme d'origine. Notamment, la topologie physique a évolué vers une étoile pour gérer la rupture de l'anneau. Les stations sont reliées à des concentrateurs (**MAU***, Multiple Access Unit*) comme le montre la figure 12.42.

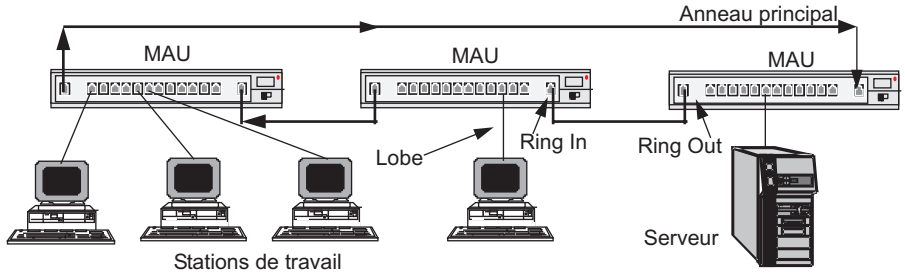


Figure 12.42 Présentation du réseau Token Ring.

Les spécifications d'installation du Token Ring sont contraignantes. Les possibilités de connexion, distance et nombre de postes, dépendent du type de câble utilisé. Avec du câble de type 1 ou 2 (dans la terminologie IBM, paires torsadées blindées d'impédance 150 Ω), la longueur maximale de l'anneau principal est de 366 m (chaque MAU comptant pour 4,9 m). Il peut comporter jusqu'à 260 stations pour une distance maximale station/MAU de 101 mètres.

Les spécifications des éléments actifs ont évolué afin de supporter le précâblage d'immeuble à 100 Ω. Le connecteur spécifique IBM dit « hermaphrodite » est aujourd'hui remplacé par des prises RJ45.

12.4.2 Principe général du jeton sur anneau

Le mécanisme du jeton

Le droit d'émettre est matérialisé par une trame particulière « le jeton ou *token* ». Celui-ci circule en permanence sur le réseau. Une station qui reçoit le jeton peut envoyer une ou plusieurs trames, elle devient station maître. Si elle n'a rien à émettre, elle se contente de répéter le jeton, elle est dite : station répéteur. Dans un tel système, les informations (trames) transitent par toutes les stations actives.

Chaque station du réseau répète le jeton ou le message émis par la station maître, il n'y a pas de mémorisation du message, un bit reçu est immédiatement retransmis. Le temps alloué à une station pour la répétition d'un bit correspond à un temps bit (possibilité de modifier bit

à bit le message). Chaque station provoque ainsi un temps bit de retard dans la diffusion d'un message.

Le jeton ne contient pas l'adresse d'un destinataire, le destinataire est la station qui suit physiquement celle qui le détient (technique du jeton non adressé). Le mécanisme du jeton est illustré par la figure 12.43.

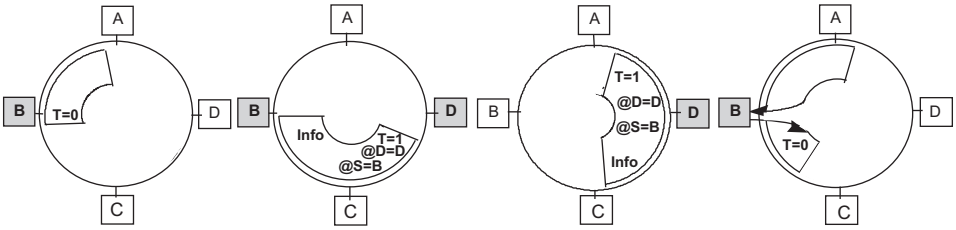


Figure 12.43 Principe du jeton.

Sur le premier schéma de la figure 12.43, la station B, qui a des données à émettre, reçoit un jeton libre. La disponibilité ou l'indisponibilité du jeton est indiquée par la valeur d'un bit : le bit T (*Token*) ; s'il est à zéro, le jeton est libre, sinon le jeton est marqué « occupé » (T = 1). La station B marque le jeton occupé (T = 1), émet à la suite du jeton son message (@Destination, @Source, informations), et devient, momentanément, le maître de l'anneau.

Pour éviter qu'une station monopolise l'anneau, le temps de détention du droit d'émission est limité. Ce temps est, par défaut, d'environ 10 ms.

La station C lit le jeton, celui-ci est marqué occupé, elle lit l'adresse destination. N'étant pas le destinataire du message, elle ne fait que régénérer le message (fonction répéteur). La station D procède de même, mais elle reconnaît son adresse et recopie, au vol, le message. B reçoit l'en-tête du message qu'il a émis. Elle l'ôte de l'anneau (ne le retransmet pas), dès qu'elle a reconnu son adresse (@Source) elle réémet un jeton libre sur le support (T = 0).

Dans la version de base, à 4 Mbit/s, un seul jeton circule en permanence sur le support (système à trame unique). Pour faire évoluer le débit à 16 Mbit/s et améliorer l'efficacité, lorsque la station maître a terminé d'émettre son message, elle régénère un jeton (système à trames multiples ou protocole **ETR**, *Early Token Release*). De ce fait, plusieurs messages d'origines différentes et un jeton libre peuvent circuler en permanence sur le réseau. Quand une station a émis, les premiers bits qu'elle reçoit sont toujours ceux qu'elle a émis, sinon il y a une erreur. Ces bits ne sont pas répétés, la station élimine tous les bits jusqu'au délimiteur de fin de trame. Elle reprend après son rôle de répéteur.

Gestion de l'anneau

➤ Format de la trame 802.5

La trame 802.5 utilise deux formats de trames, les trames dites LLC pour le transport d'information et les trames dites MAC pour la gestion de l'anneau). Dans une trame MAC, le champ d'information est vide. La trame 802.5 est représentée figure 12.44.

Quatre octets spécifiques de la trame MAC 802.5 distinguent les différentes fonctions et permettent la gestion de l'anneau. Ce sont : l'octet de contrôle d'accès (*Access Control*), l'octet

© Dunod – La photocopie non autorisée est un délit

de contrôle de trame (*Frame Control*), l'octet de fin de trame (*End Delimiter*) et enfin, l'octet d'état de la trame (*Frame Status*).

SD	AC	FC	DA	SA	RI	Données	FCS	ED	FS
JK0JK000	PPPTMRRR		6octets	6 octets	2 à 30 octets		4 octets	JK1JK1IE	ACrrACrr

Figure 12.44 La trame IEEE 802.5.

➤ L'octet de contrôle d'accès (AC, *Access Control*)

L'octet de contrôle d'accès comporte quatre champs (figure 12.45).

PPP	T	M	RRR

Figure 12.45 Octet de contrôle d'accès.

Le bit **T** : l'état du jeton est matérialisé par la valeur du bit T (*Token*). Quand le token est à zéro (T = 0) le jeton est libre et la station qui le détient peut transmettre un message. À un (T = 1), le jeton est occupé et un message suit.

Le bit **M** : le bit M (Moniteur) est toujours à zéro dans un jeton libre et dans le message émis par la station émettrice. Il est positionné à 1 par une station particulière : le moniteur. Cette station a pour rôle de surveiller qu'un message ne boucle pas sur le réseau (trame orpheline). À cette fin, quand le moniteur voit passer un message, il examine la valeur du bit M. S'il est à zéro, il le passe à 1. S'il est à un, c'est que le message boucle, il aurait dû être retiré par la station émettrice. Le moniteur va dans ce cas, suppléer la station défaillante et régénérer un jeton libre (au tour suivant).

La station moniteur a un rôle très particulier :

– elle synchronise le réseau. C'est la seule station dont les horloges émission et réception sont séparées. Toutes les autres stations du réseau sont synchronisées sur l'horloge d'émission du moniteur (réseau synchrone) ;
– elle garantit la présence d'un jeton valide en supprimant les trames orphelines, en régénérant un jeton de plus faible priorité, lorsqu'une même priorité monopolise le jeton. À chaque passage de jeton valide, elle arme un temporisateur ; à l'échéance de celui-ci, elle considère que le jeton est perdu, purge l'anneau (envoi d'une trame particulière) et insère un nouveau jeton valide ;
– elle assure une contenance minimale à l'anneau (*ring latency*) en introduisant un retard de 24 bits, garantissant ainsi que l'anneau contient au moins le jeton.

Toutes les stations ont vocation à être moniteur, mais une seule à la fois remplit ce rôle. Le moniteur actif signale, périodiquement (toutes les 7 s), sa présence par une trame particulière (Trame MAC : *Active_Mo*nitor). Cette trame déclenche une série d'actions, notamment l'envoi, par chaque station, d'une trame MAC signalant sa présence (*Standby_Monitor_Present*) permettant à chaque station d'apprendre l'adresse de sa précédente. Ce mécanisme permet de vérifier la continuité de l'anneau.

Cependant, toutes les stations participent à la surveillance de l'anneau. À chaque réception d'un jeton libre, elles arment un temporisateur. À l'échéance de celui-ci (15 s), la station consi-

dère qu'il n'y a pas de moniteur actif sur le réseau et déclenche une procédure de recherche de jeton (*Claim_Token*, trame de candidature). À réception d'une trame *Claim_Token*, chaque station examine le champ adresse si celle-ci est inférieure à la sienne, elle y inscrit sa propre adresse et devient ainsi candidate. Si la trame *Claim_Token* revient à la station candidate avec sa propre adresse, cette dernière devient station moniteur actif et génère un jeton valide.

Les bits **PPP** et **RRR** : la norme 802.5 prévoit huit niveaux de priorité (3 bits). Lorsqu'une station veut émettre, elle attend le jeton. Si celui-ci est occupé, elle le réserve en positionnant les bits RRR (niveau de réservation). Si les bits sont déjà positionnés, la station n'en modifie la valeur que si le niveau requis est supérieur à celui de la réservation déjà effectuée. Dans ce dernier cas, elle mémorise l'ancien niveau de priorité.

La station qui purge l'anneau, émet un jeton de la priorité (PPP) égale à la demande de réservation mémorisée (RRR). Une station ne peut prendre le jeton que si les données qu'elle a à émettre sont d'une priorité au moins égale à PPP. Si une station intercepte le jeton (priorité plus grande ou égale à PPP), elle mémorise le niveau du jeton (PPP). Lorsque la station libérera le jeton, elle le régénérera avec la priorité mémorisée.

➤ L'octet de contrôle de trame (FC, *Frame Control*)

L'octet de contrôle de trame du réseau 802.5 définit le type de trame qui circule sur l'anneau. Les deux premiers bits distinguent les trames d'information (trames LLC) des trames de gestion de l'anneau (trames MAC). Le tableau de la figure 12.46 donne la signification des différentes combinaisons binaires.

Frame Control		Type de trame	Fonction
00		MAC	
	000 000 000 010 000 011 000 100 000 101 000 110	Test duplication d'adresse Beacom Claim Token Purge de l'anneau Moniteur actif présent (AMP) Standby Moniteur présent (SMP)	Teste si deux stations ont la même adresse Localisation d'une station défaillante Élection d'un moniteur Initialisation de l'anneau Utilisé par le moniteur pour signaler sa présence Utilisé par chaque station pour signaler sa présence
01		Trame LLC (Data)	
	000 PPP	Priorité de la trame	Transfert de données

Figure 12.46 Signification de l'octet de contrôle de trame.

➤ L'octet de fin de trame (ED, *End Delimiter*)

Le positionnement à 1 du bit **I** de l'octet délimiteur de fin de trame (figure 12.47) informe le destinataire qu'une trame de même origine suit celle reçue, à 0 il indique que la trame est unique ou la dernière d'un envoi. Le bit **E** positionné à 0 par l'émetteur est basculé à 1 par la première station qui détecte une erreur ; il n'est plus modifié par la suite. Le protocole IEEE 802.5 utilise le codage Manchester différentiel. Les symboles J et K ne sont ni des 1 ni des 0, ce sont des éléments binaires sans transition au milieu du temps bit (violation de la loi de codage Manchester).

© Dunod – La photocopie non autorisée est un délit

Figure 12.47 Octet de fin de trame.

➤ L'octet d'état de la trame (FS, *Frame Status*)

L'octet d'état de la trame (figure 12.48) est le dernier octet de la trame. Non protégé par le FCS, ses informations sont dupliquées. Les bits « r r » sont réservés à un usage ultérieur. Le bit A est positionné à 1 par la station qui a reconnu sa propre adresse dans le champ adresse destination. Cette station, si elle a correctement recopié la trame (accusé de réception), positionne à 1 le bit C.

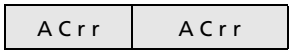


Figure 12.48 Octet d'état de la trame.

➤ Le champ RI

D'origine IBM, le routage par la source (*Source Routing*) est un mode de fonctionnement spécifique des ponts[9] dans l'environnement Token Ring. Les ponts, éléments d'acheminement de niveau 2, n'entretiennent aucune table d'acheminement. Ils se contentent de router les trames selon les indications contenues dans le champ d'informations de routage (**RI**, *Routing Information*) de la trame Token Ring. La notion d'adresse source MAC de diffusion n'ayant aucun sens, le bit multicast de ce champ valide le champ RI. Si le bit de diffusion est 0 : pas de champ RI, bit à 1 : présence du champ RI. La figure 12.49 représente une trame MAC comportant des informations de routage.

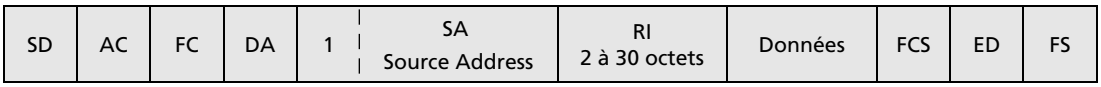


Figure 12.49 Trame MAC validant le champ RI.

Dans le *Source Routing*, ce sont les stations et non les ponts qui entretiennent les tables d'acheminement. Ces tables peuvent être statiques (initialisées par l'administrateur) ou dynamiques (construites par la station).

Le champ RI (figure 12.50), d'un maximum de 30 octets, contient les informations suivantes :

– **type de trame**, sur 3 bits ce champ identifie la nature de la trame :
  – 001, trame d'information à acheminer selon les informations contenues dans le champ RI ;
  – 010, trame d'apprentissage, cette trame est diffusée par une station qui désire connaître le chemin pour joindre une autre station,

9. Voir section 14.3.5.

  - 100, trame d'apprentissage, celle-ci n'emprunte que les branches établies, précédemment, par le *Spanning Tree Protocol*[10] ;
- **longueur**, ce champ, de 5 bits, spécifie la longueur du champ RI (32 octets maximum) ;
- **sens**, ce bit indique si la route à suivre doit être lue de gauche à droite ou de droite à gauche ;
- **MTU** (*Maximum Transfer Unit*), ce champ de 4 bits indique la taille maximale des unités de données qui peuvent être transférées sur le réseau traversé, les valeurs sont codifiées (576, 1500, 2052, 4472, 8144, 11407, 17820, 65535) ;
- enfin, le champ **route** qui contient *n* sous-champs *Route Designator*. Le sous-champ *Route Designator* sur 16 bits identifie le réseau, ou port, sur 12 bits et le pont traversé sur 4 bits. Les identificateurs sont initialisés par l'administrateur de réseau.

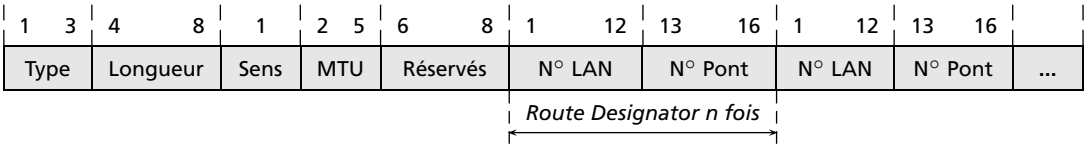


Figure 12.50 Structure du champ RI.

12.4.3 Comparaison Ethernet/Token Ring

Lorsque l'on compare deux types de réseaux, les critères à retenir sont principalement :

- les performances en termes de débit et temps d'accès ;
- les types de transferts et applications informatiques envisageables ;
- l'infrastructure requise et les distances maximales admissibles ;

En termes de débit et temps d'accès

Le débit d'un réseau peut s'exprimer selon 3 valeurs. Le **débit nominal** qui correspond au débit physique sur le lien. Le **débit utile** qui représente les données effectivement transmises sur le réseau, tandis que le **débit effectif** correspond à celui vu des applications. Le premier est effectivement lié au choix du réseau, le second dépend non seulement du débit physique mais aussi de la charge du réseau et des protocoles empilés. Seuls, nous intéressent ici les débits nominaux et la tenue en charge du réseau (débit utile).

La figure 12.51 superpose l'évolution des débits en fonction de la charge de chaque réseau. Il est intéressant de constater qu'à faible charge, les réseaux de type Ethernet présentent, vis-à-vis des couches supérieures, une meilleure efficacité. En effet, en Ethernet, si le trafic est faible, dès qu'une station veut émettre, elle émet. En *Token Ring*, même à faible charge, la station doit attendre le jeton.

Cependant, à forte charge dans le réseau Ethernet, les collisions se multiplient et le débit utile sur le support s'effondre, alors que dans le cas du réseau *Token Ring*, même si le débit effectif de chaque station diminue, le débit utile sur le support tend vers le débit nominal.

10. Voir section 14.3.4.

© Dunod – La photocopie non autorisée est un délit

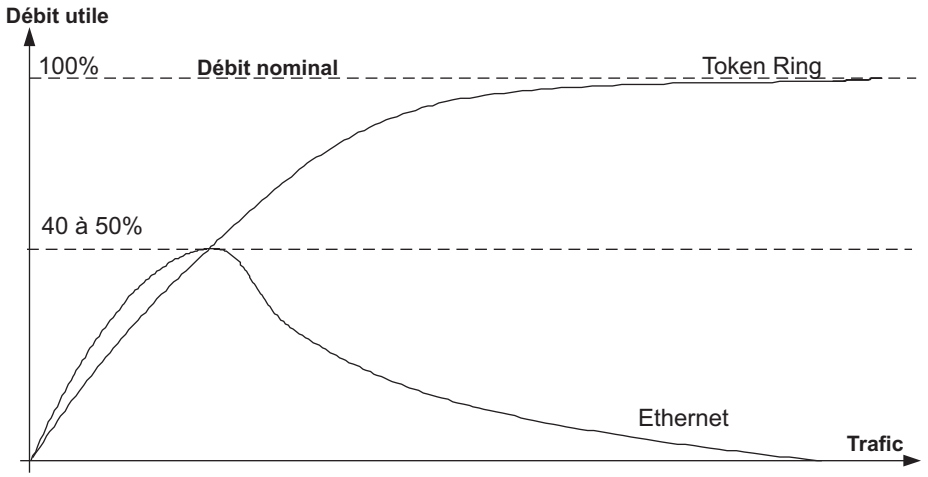


Figure 12.51 Courbe de comparaison Ethernet/Token Ring.

En termes d'application

Le réseau Ethernet est qualifié de probabiliste, c'est-à-dire qu'il est possible de déterminer, en fonction d'un trafic modélisé, la probabilité pour qu'une station puisse émettre. Il est impossible de borner ce temps. Dans le cas du Token Ring, il est toujours possible de déterminer le laps de temps au bout duquel on est certain qu'une station obtiendra le jeton, le réseau est dit déterministe (à priorité constante).

Cependant, même si le temps d'obtention du jeton peut être borné, même si le *Token Ring* met en œuvre un mécanisme de priorité, il ne peut garantir un intervalle de temps constant entre deux obtentions du jeton par une même station. Par conséquent, le *Token Ring* est impropre au transfert isochrone (voix, vidéo temps réel).

Les deux types de réseaux sont utilisés pour des applications de type conversationnel (trafic sporadique). Le *Token Ring*, pouvant garantir une bande minimale, pourra être utilisé pour des transferts sous contrainte temporelle légère. En principe, aucun des deux ne satisfait aux contraintes du transfert isochrone. En pratique, des essais ont montré qu'il était possible, sous faible charge, de réaliser de tels transferts, à condition d'admettre des pertes d'information pour assurer une compensation temporelle.

En termes d'infrastructure

Si on ne considère que l'implémentation la plus utilisée du réseau Ethernet : le 10 et 100 base T, la topologie physique de câblage est similaire pour les deux types de réseaux. Les distances couvertes sont du même ordre. Ces deux réseaux permettent de couvrir des immeubles relativement vastes en utilisant les techniques de réseaux fédérateurs. Ces techniques, succinctement illustrées par la figure 12.52, seront étudiées au chapitre suivant.

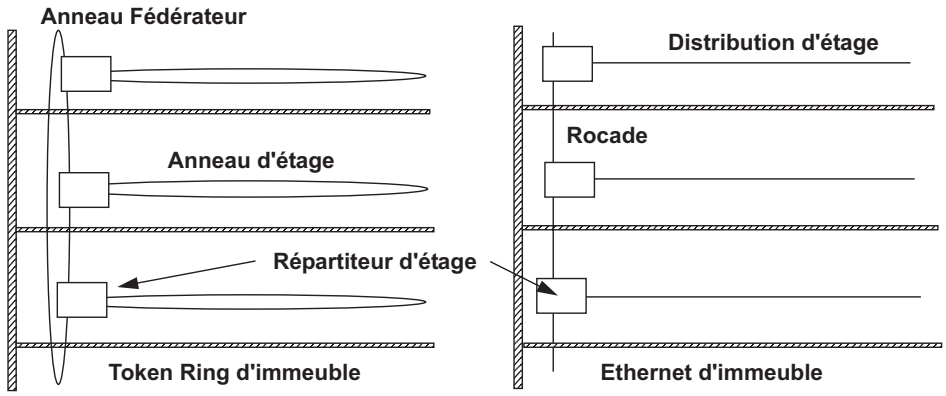


Figure 12.52 Interconnexion de réseaux d'étage par un réseau fédérateur.

Conclusion

Bien que le réseau Token Ring ait des performances intrinsèquement supérieures, le marché lui a préféré Ethernet. Deux raisons essentielles expliquent ce succès. La première est essentiellement économique, la facilité d'implémentation du protocole CSMA/CD a permis la réalisation d'adaptateurs beaucoup moins chers que ceux du 802.5. La seconde, d'ordre technique, réside dans la possibilité de faire cohabiter, sur un même réseau le 10 et le 100 Mbit/s. Cette dernière facilité a autorisé des migrations de parcs en douceur et a définitivement consacré la suprématie d'Ethernet.

12.5 LE JETON ADRESSÉ OU TOKEN BUS, IEEE 802.4

12.5.1 Généralités

Réseau industriel, le *Token Bus* est aujourd'hui le seul réseau sur support filaire qui utilise un canal large bande (figure 12.53). Conçu pour fonctionner en milieu industriel, le *Token Bus* utilise du câble coaxial (CATV de 75 Ω), les débits possibles sont 1, 5 et 10 Mbit/s.

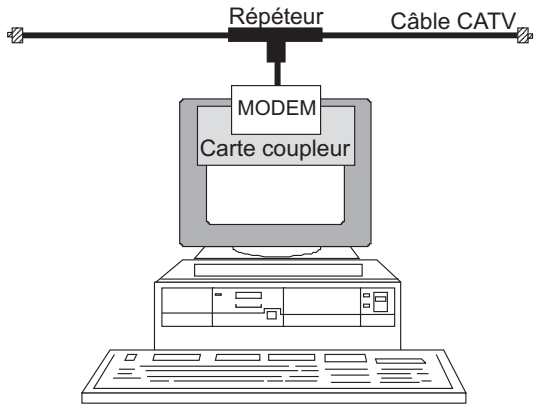


Figure 12.53 Niveau physique du IEEE 802.4.

© Dunod – La photocopie non autorisée est un délit

Le protocole IEEE 802.4 est mis en œuvre dans le réseau **MAP** (*Manufacturing Automation Protocol*).

12.5.2 Fonctionnement du jeton sur bus

Principe

Dans la technique d'accès « *jeton adressé sur bus* », le jeton, circule de la station de plus faible adresse à celle de plus forte adresse, formant ainsi un anneau virtuel sur le bus (anneau logique/bus physique). Dans le système, représenté figure 12.54, chaque station, à tour de rôle, reçoit le jeton. Si elle a des données en attente d'émission, elle les émet, puis passe le jeton à la station suivante (celle dont l'adresse suit la sienne).

Toutes les stations en fonctionnement sur le réseau perçoivent le message (bus), mais seule celle dont l'adresse est contenue dans le jeton, considère l'avoir reçu (jeton adressé). Si elle n'a rien à émettre, elle transfère immédiatement le jeton à la station suivante.

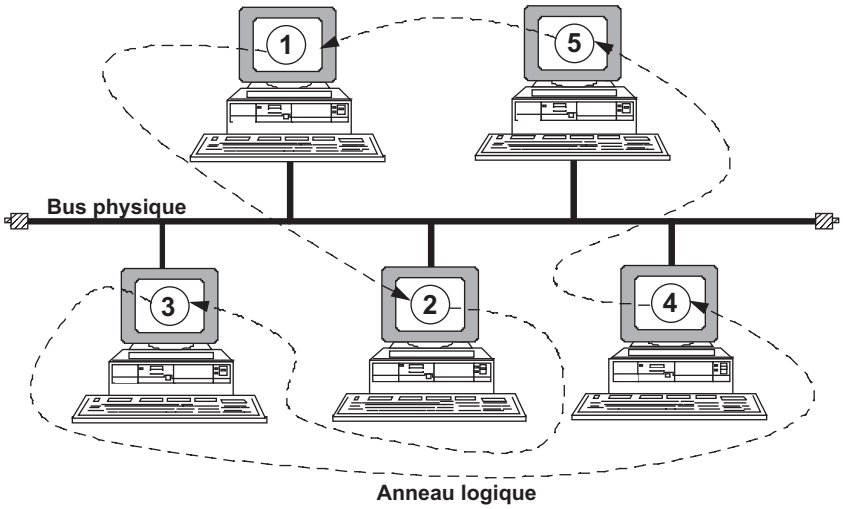


Figure 12.54 Principe du bus à jeton.

Cet algorithme impose que chaque station connaisse l'adresse de celle qui la suit sur l'anneau (**NS**, *Next Station address*) et de celle qui la précède (**PS**, *Previous Station address*). Se pose alors le problème de l'apprentissage, de l'insertion et du retrait d'une station.

Gestion de l'anneau

➤ Initialisation de l'anneau et perte du jeton

La perte du jeton ou l'initialisation de l'anneau sont traitées de manière identique. La procédure d'initialisation ou de réinitialisation est déclenchée par détection d'inactivité sur le support (timer d'inactivité remis à zéro à chaque détection d'activité). La station qui détecte l'inactivité passe en procédure d'appel du jeton (trame *claim token*).

La station émet alors une trame *claim token* dont la longueur est une fonction de son adresse, puis, elle passe en écoute. Si elle détecte une activité elle abandonne, sinon elle réitère. Lorsque

le silence persiste, elle se considère comme propriétaire du jeton et entreprend la procédure d'insertion pour reconfigurer l'anneau. Notons que cette procédure donne le jeton à la station de plus grande adresse (temps d'émission le plus long).

➤ Insertion d'une station sur le réseau

Une station ne peut s'insérer dans l'anneau que si elle y est invitée par la station dont elle doit devenir le successeur sur l'anneau. À cet effet, la station qui détient le jeton déclenche périodiquement une procédure de réveil. La procédure de réveil est déclenchée tous les N passages de jeton. N compris dans l'intervalle [16, 255] est un paramètre défini par l'administrateur du réseau. La figure 12.55 illustre le mécanisme d'insertion.

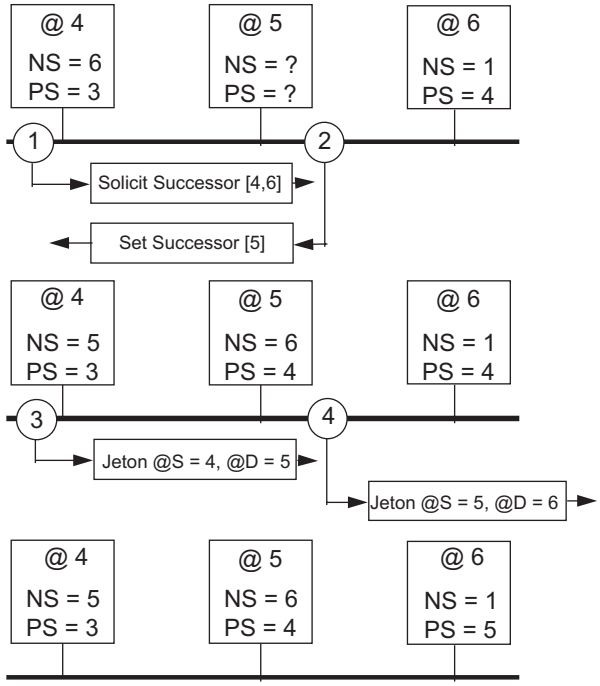


Figure 12.55 Insertion d'une station.

La station 5 (que nous supposerons d'adresse 5 notée : @5) attend pour s'insérer de recevoir une invitation à le faire. Celle-ci est matérialisée par une trame particulière « *solicit successor* » dont l'adresse source et destination définissent l'intervalle d'insertion. Ce message (étape 1) invite les stations, dont l'adresse est comprise entre celle de la station origine de l'invitation et sa suivante actuelle, à se manifester. Une réponse est attendue pendant un *time slot*.

La station 5, détectant que son adresse (@5) est dans l'intervalle d'insertion, répond par le message « *set successor* » et met à jour ses variables NS et PS (étape 2). La station 4 apprend ainsi que son nouveau successeur est la station 5 et lui envoie le jeton (étape 3). La station 5 transmet alors le jeton à sa suivante qui apprend ainsi que la station 5 est sa nouvelle précédente (étape 4).

Si plusieurs stations sont comprises dans l'intervalle d'insertion, elles répondent simultanément provoquant ainsi une collision sur le bus. La station origine de la trame d'insertion

© Dunod – La photocopie non autorisée est un délit

détecte la collision et met en œuvre un algorithme de résolution des contentions. Pour cela, elle émet une trame, *resolve contention*, cette trame définit un temps d'attente de 4 time slot.

Ne peut (ou ne peuvent) répondre pendant le premier intervalle de temps que la (ou les) station(s) dont les deux premiers bits d'adresse sont 00, pendant le second celles dont les deux premiers bits d'adresse sont 01, puis 10 enfin 11. Dès qu'une station a répondu les autres ne répondent plus. La procédure d'insertion ne permet l'insertion que d'une seule station à la fois. Si de nouvelles collisions se produisent le mécanisme est repris, mais avec les deux bits suivants de l'adresse et ainsi de suite. Pour limiter le risque de collisions, seules les stations ayant participé à la collision précédente peuvent répondre à la trame *resolve contention*.

➤ Retrait d'une station du réseau

Une station qui désire se retirer de l'anneau envoie, lorsqu'elle dispose du jeton, une trame *set successo*r à sa précédente et le jeton à sa suivante, avec l'adresse source de sa précédente. Chaque station peut ainsi mettre ses variables à jour et la continuité de l'anneau est préservée (retrait normal d'une station).

Une station peut aussi se retirer anormalement de l'anneau (panne, arrêt intempestif...). L'anneau est alors rompu. Lors du passage du jeton, l'émetteur écoute le support, s'il ne détecte aucune activité, c'est-à-dire que son successeur ne retransmet pas le jeton, il réémet le jeton. Si de nouveau il ne détecte aucune activité, il émet une trame « *who follows* » (qui suit ?). Celle-ci contient l'adresse de la station défaillante (celle qui était destinataire du jeton et qui n'a pas répondu) et sa propre adresse.

La station qui reconnaît dans l'adresse destination (adresse de la station défaillante) l'adresse de sa station précédente, met à jour sa variable **PS** (station précédente) avec l'adresse de la station source et émet une trame *set successor*. La station défaillante est court-circuitée. Elle doit de nouveau attendre un polling d'insertion pour s'insérer dans l'anneau.

➤ Priorité

Le protocole IEEE 802.4 prévoit un mécanisme optionnel de priorité à 4 classes. Chaque station tient à jour un timer **TRT** (*Token Rotation Timer*). Pour chaque niveau de priorité, un temps maximal de rotation du jeton est défini (**TTRT**, *Target Token Rotation Time*). Si la station a des données à émettre, elle compare son TRT au TTRT correspondant au niveau de priorité des données à transmettre. Si TRT < TTRT, elle transmet dans les limites du TTRT, sinon elle diffère son émission.

Le réseau *Token Bus* est utilisé en environnement industriel, il autorise le temps réel à condition d'inhiber le mécanisme d'insertion de stations.

12.5.3 Format des données

La trame MAC 802.4 (figure 12.56) comporte :

– un champ préambule d'au moins un octet et d'une durée minimale de 2 μs ;

– des délimiteurs assurent la synchronisation caractère (**SD**, *Start Delimiter*), le marquage de fin de trame, et signalent éventuellement une erreur selon en positionnant du bit **E** du *End delimiter* ;

– l'octet de contrôle de trame (**FC**, *Frame Control*) indique le type de trame (jeton, données...) ;
– les champs d'adresse spécifient les adresses destination (DA) et source (SA) ;
– le champ de données peut contenir de 0 à 8 191 octets ;
– enfin, le FCS protège les champs FC, DA, SA et données.

Préambule	SD Start Delimiter	FC Frame Control	DA Destination Address	SA Source Address	Information 0 à 8 181 octets	FCS	ED End Delimiteur

Figure 12.56 Trame IEEE 802.4.

12.6 LE RÉSEAU 100 VG ANY LAN, 802.12

12.6.1 Généralités

D'origine HP et AT&T et normalisé par le groupe de travail IEEE 802.12, le 100 VG *Any Lan*[11] implémente un nouveau protocole d'accès fondé sur la méthode du polling. Les trames peuvent être au format Ethernet ou Token Ring, selon la configuration, d'où l'appellation *d'Any Lan*. Se contentant de simples paires torsadées de qualité vocale (**VG**, *Voice Grade*), le 100 VG *Any Lan* offre un débit de 100 Mbit/s et un accès déterministe. Il admet du trafic de type isochrone.

Les distances couvertes dépendent du type de câble utilisé. Elles sont de 100 m (hub/station ou hub/hub) avec du câble catégorie 3 (*Voice Grade*) et catégorie 4. Elles atteignent 150 m (voire 200 m) avec du câble catégorie 5 UTP (non blindé, *Unshielded Twisted Pair*).

Le réseau 100 VG *Any Lan*, en raison de son protocole d'accès, utilise au maximum la bande passante (bande utile de 80 Mbit/s contre 40 à 50 Mbit/s pour l'Ethernet). Concurrent malheureux de l'Ethernet 100 Mbit/s, le 802.12 est resté très confidentiel. Seule, la description de sa méthode d'accès justifie son étude.

12.6.2 Le DPAM

Principe

Les stations sont raccordées à un concentrateur intelligent selon une topologie physique identique à celle du réseau 10 base T (réutilisation du câblage existant). Lorsqu'une station a des données à émettre, elle formule une requête au hub, qui lui alloue ou non le support (*Demand Priority Access Method* ou **DPAM**).

Les schémas de la figure 12.57 illustrent succinctement le principe de DPAM :
– Le hub informe les stations et celles-ci informent le hub de leur disponibilité (émission du signal *IDLE*).
– La station ayant des données à émettre le signale au hub en lui envoyant une requête selon

11. Le 100 VG LAN est une proposition commune d'Heweltt Packard, IBM et d'AT&T.

© Dunod – La photocopie non autorisée est un délit

le niveau de priorité des données. Ici, ce sont des données de priorité normale, signal **NPR** (*Normal Priority Request*).

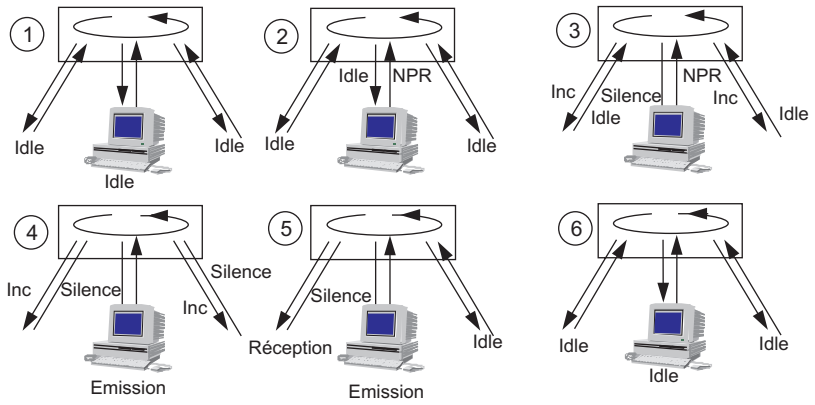


Figure 12.57 Principe du DPAM.

– Le hub scrute en permanence ses différents ports (*round robin*). Durant cette phase de polling, le hub détecte la demande de la station. Il informe les autres stations qui lui sont raccordées de se mettre en état de recevoir (signal *Incoming*, **INC**) et cesse son émission de Idle vers la station demanderesse (silence).
– Les stations signalent au hub qu'elles sont prêtes à recevoir en cessant leur émission de Idle. La station demanderesse interprète la non-réception de Idle comme une autorisation d'émettre, elle transmet sa trame.
– Le hub, à réception de cette dernière, examine l'adresse destination et retransmet la trame sur le seul port intéressé. Ce processus nécessite l'implémentation d'un protocole d'apprentissage d'adresses. Le hub reprend, vers les autres stations, l'émission de Idle.
– À la fin du cycle, après émission et réception de la trame toutes les stations et le hub émettent les signaux Idle.

Principe de la signalisation

Tonalité	Hub vers station		Station vers Hub	
Silence	Prêt à émettre ou à recevoir			
1 et 1	IDLE	Rien à envoyer	IDLE	Rien à transmettre
1 et 2	Incoming INC	Demande de passage en état réception	NPR	Requête de priorité normale
2 et 1			HPR	Requête de priorité haute
2 et 2	Initialisation INIT	Signal d'initialisation, déclenché notamment pour l'apprentissage des adresses MAC des stations raccordées à un HUB.		

Figure 12.58 Signalisation du réseau 100 VG *Any Lan*.

La signalisation utilisée dans les différentes phases du processus décrit précédemment est réalisée à partir de l'émission continue de signaux de fréquences différentes (0,9375 MHz pour

la tonalité 1 et 1,875 MHz pour la tonalité 2). Ces signaux sont émis sur des paires différentes ou, selon le support physique utilisé, multiplexés. Le tableau de la figure 12.58 détaille les différentes combinaisons et les actions qu'elles déclenchent.

Performance

Le principe utilisé garantit que chaque station pourra avoir accès au support. Il est aisé de déterminer ce temps, il correspond au temps d'émission de chaque station multiplié par le nombre de stations. *Any Lan* implémente un mécanisme de priorité à deux niveaux : les données normales et les données prioritaires, les données prioritaires sont toujours émises avant les données normales.

Afin d'éviter qu'une station ne monopolise l'émission, par un usage abusif des données prioritaires, le hub surveille la file d'attente des requêtes de données normales. À l'échéance d'un timer (**TTT**, *Target Transmission Time*), les demandes normales, non satisfaites, sont classées en priorité haute. De ce fait, la borne haute du délai d'émission est $n \bullet TTT$ ou n est le nombre de stations.

12.7 LA COMMUTATION DANS LES LAN

12.7.1 Principe de base

Issue de la téléphonie et des réseaux grande distance (**WAN**), puis mis en œuvre dans le monde Ethernet (*Switched Ethernet*) pour résoudre les problèmes d'effondrement des réseaux (collisions) et garantir une certaine bande passante, la technique de commutation est aujourd'hui largement utilisée pour réaliser tout type de réseaux. Traditionnellement, la commutation consiste à mettre en relation directe un port d'entrée avec un port de sortie, la relation étant établie préalablement à toute communication par un protocole de signalisation.

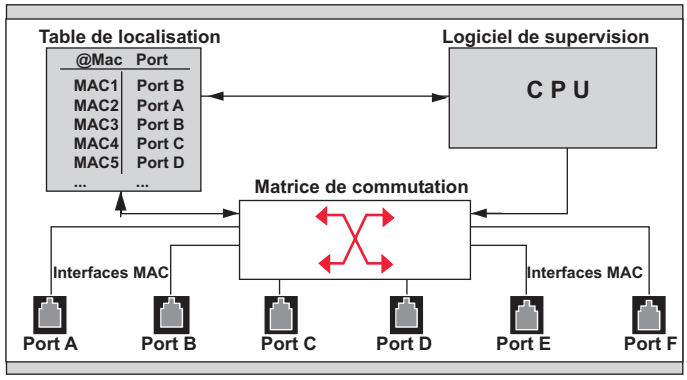


Figure 12.59 Principe d'un commutateur.

La commutation dans les réseaux locaux, n'ouvre pas explicitement un circuit virtuel. Le commutateur établit dynamiquement (commutation dynamique) une table de localisation ou d'acheminement (figure 12.59). Pour construire cette table, le commutateur examine le trafic reçu par chacun de ses ports. La table d'acheminement (**FDB**, *Forwarding Data Base*) est construite par examen des adresses MAC sources. Le commutateur apprend ainsi la locali-

© Dunod – La photocopie non autorisée est un délit

sation géographique des stations. À réception d'une trame, le commutateur consulte la table d'acheminement (table de commutation) et achemine la trame reçue sur le seul port où est localisé le destinataire. Les trames à destination d'une adresse non inscrite dans la table et celles de diffusion sont répétées sur tous les ports, sauf le port de réception. Les tables ne peuvent posséder autant d'entrées que de stations connectées. Aussi, périodiquement, les adresses les plus anciennes sont effacées. À cet effet, on associe, à chaque entrée de la table, un temporisateur. Le temporisateur est réinitialisé à chaque réception d'une trame de même origine, à échéance l'entrée est effacée.

12.7.2 Notion d'architecture des commutateurs

Historiquement, dans les premiers commutateurs spatiaux, des relais électromagnétiques mettaient en relation un circuit d'entrée avec un circuit de sortie (commutateur crossbar), par la suite, les relais furent remplacés par des semi-conducteurs (transistors). Le principe des commutateurs crossbar est représenté figure 12.60. À chaque croisement, un transistor établit ou rompt la liaison entre les deux conducteurs. Les points « noirs » de la figure schématisent l'état passant des transistors et donc la relation entre les conducteurs, les points « clairs » représentent l'état bloqué du transistor et donc la coupure entre les deux circuits.

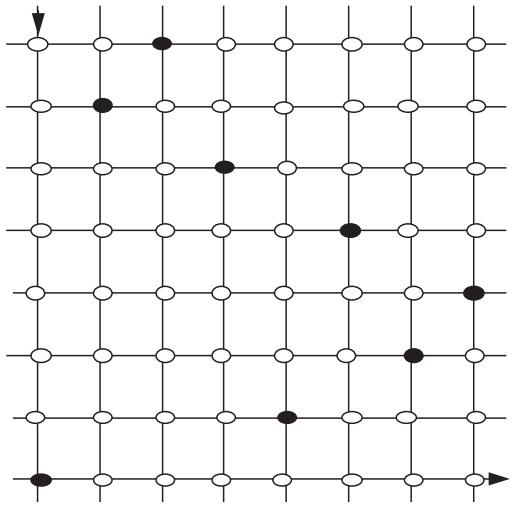


Figure 12.60 Principe d'une matrice de type crossbar.

Autorisant le parallélisme dans le traitement des trames, les commutateurs de type crossbar sont très efficaces mais aussi très complexes ; le nombre de points de connexion évolue en N^2 où N représente le nombre de ports. Une solution à cette complexité est fournie par les commutateurs multiétage dont la réalisation la plus courante est le commutateur Banyan. Les commutateurs du type Banyan ne comportent que $N \cdot \text{Log}\, N$ composants. La figure 12.61 illustre le principe de mise en relation d'un port d'entrée avec n'importe quel port de sortie. Chaque port d'entrée de ce système peut être mis en relation avec tout port de sortie.

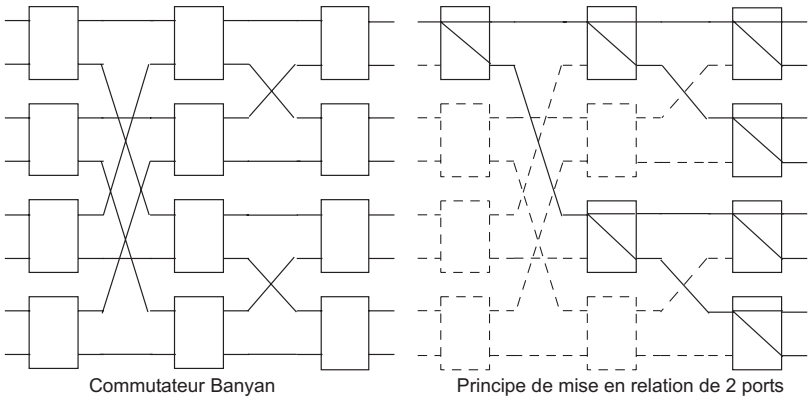


Figure 12.61 Principe d'un commutateur de type Banyan.

Ces architectures répondent mal au problème de la diffusion. Aussi, des architectures, certes peut-être moins efficaces que celles du type Banyan mais beaucoup simples, ont la faveur des constructeurs. Ce sont les architectures à bus et à mémoire partagée. La première correspond à la réalisation d'un réseau très haut débit (*collapsed backbone*). Le débit du bus devant être au moins égal à la demi-somme des débits incidents. La seconde solution, la plus courante, est celle de la mémoire partagée à accès multiples simultanés. Toutes les trames sont recopiées en mémoire centrale avant d'être commutées. Ce dernier type d'architecture permet de résoudre simplement les mécanismes de blocage.

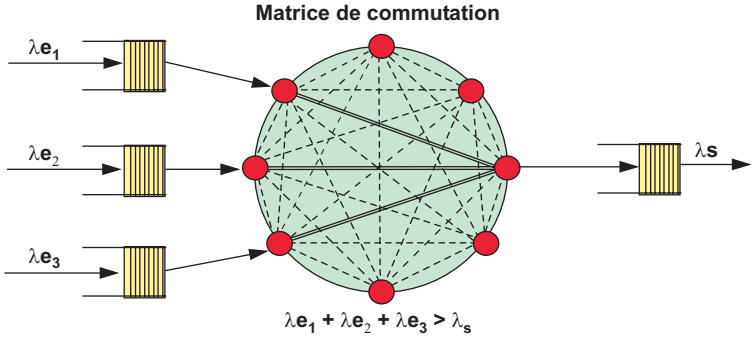


Figure 12.62 Congestion dans les commutateurs.

Un commutateur peut mettre en relation n'importe quel port d'entrée avec n'importe quel port de sortie. Si simultanément, plusieurs flux d'entrée doivent converger vers un même port de sortie, il peut y avoir dépassement des capacités d'émission du port de sortie et pertes de données. Afin d'éviter ces pertes, le système est doté de buffers d'attente. Les commutateurs peuvent disposer exclusivement de buffers d'entrée ou de sortie. En cas de conflit d'accès à un port de sortie, si le système ne possède que des buffers en entrée, il peut se produire un blocage en entrée (perte de cellules). Si le système n'est doté que de buffers de sortie, on ne peut exclure un blocage en entrée que si les buffers de sortie sont suffisamment dimensionnés pour admettre une convergence de tous les flux d'entrée vers un unique port de sortie. Cette solution conduit à la réalisation de buffers de grande taille. Dans ces conditions, les constructeurs adoptent généralement une solution mixte : buffers en entrée et buffers en sortie (figure 12.62).

© Dunod – La photocopie non autorisée est un délit

12.7.3 Les différentes techniques de commutation

La commutation améliore la gestion de la bande passante en ne mettant en relation que les ports intéressés par la communication. L'acheminement s'effectue au niveau MAC, ce qui autorise des performances élevées. Deux techniques de base sont mises en œuvre : lecture de l'adresse au vol et commutation rapide (*fast forward* ou *cut through*) ou stockage avant retransmission (*store and forward*), ce qui autorise un contrôle d'erreur, ne sont alors retransmises que les trames non erronées.

La première technique est plus performante en terme de nombre de trames commutées par seconde (faible temps de latence). Cependant, elle propage les trames erronées et en particulier les trames ayant subi une collision. Les trames de collisions sont repérables : leur longueur est inférieure à la fenêtre de collision. Pour éviter une telle propagation, le commutateur ne retransmet une trame qu'après avoir reçu 64 octets. Cette gestion augmente le temps de traitement de la durée de la fenêtre de collision (5,12 µs à 100 Mbit/s).

L'*adaptative error free* combine les deux techniques. Initialement en mode *cut throug*, si le taux d'erreur atteint un seuil prédéterminé, le commutateur bascule en mode *store and forward*.

12.7.4 Les différents modes de commutation

La configuration du système peut être statique (les tables de commutation sont introduites par l'administrateur, rare) ou dynamique (les tables de commutation sont construites par analyse de trafic et apprentissage des adresses MAC, le cas le plus général). Le commutateur peut mettre en relation des stations (commutation par port) ou des segments de réseaux (commutation de segment). La figure 12.63 illustre ces différents types.

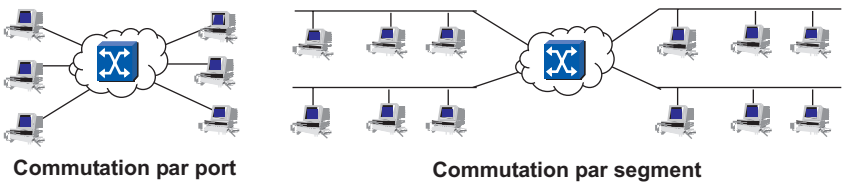


Figure 12.63 Les différents modes de commutation.

La combinaison des différentes techniques conduit à considérer quatre modes de commutations :

– la commutation statique par port permet de résoudre essentiellement les problèmes liés aux modifications fréquentes de réseau (brassage électronique depuis une console d'administration) ;

– la commutation statique par segment autorise la réalisation de différents réseaux interconnectés (segments), cette technique préserve la bande passante lors de l'accroissement des réseaux ;

– la commutation dynamique par port garantit à chaque station un débit maximal, son utilisation est préconisée pour les applications gourmandes en bande passante, elle permet les transferts isochrones entre stations Ethernet. La commutation dynamique par port assimile le commutateur à un hub ;

– la commutation dynamique par segment permet, dans une infrastructure existante (réseaux d'étage), de garantir à chaque sous-réseau (segment) un accès sécurisé, au débit nominal du raccordement, à un ou plusieurs serveurs collectifs (applications clients/serveurs, messagerie...). La commutation dynamique par segment prend en compte les sous-réseaux existants et assure une relation interdomaine sans intervention de l'administrateur. Le fonctionnement est similaire à celui d'un pont.

12.7.5 Ethernet Full Duplex

Dans la commutation par port, les risques de collision sont inexistants. L'adaptateur peut alors émettre et recevoir simultanément des messages différents, l'échange est *full duplex*. La technologie *full duplex* (**FDSE**, *Full Duplex Switched Ethernet*) permet de doubler la bande passante d'un réseau local. Initialement réservée aux liens intercommutateurs, la technologie *full duplex* est aujourd'hui supportée par la plupart des adaptateurs. Il suffit pour cela d'invalider la détection de collision. À l'instar de la commutation Ethernet, cette technique a été transposée aux réseaux Token Ring.

12.8 LES RÉSEAUX VIRTUELS OU VLAN

12.8.1 Principes généraux des VLAN

Application directe de la commutation statique, les VLAN (*Virtual Local Area Network*) autorisent, sur un même réseau physique la réalisation de plusieurs réseaux logiques totalement indépendant les uns des autres. La communication n'est autorisée qu'entre machines d'un même VLAN. Les communications inter-VLAN doivent transiter par un routeur.

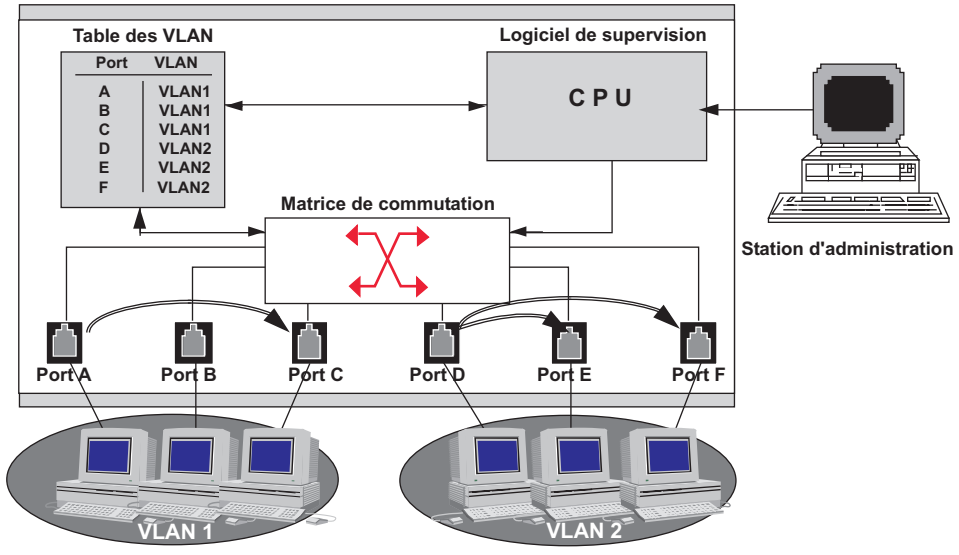


Figure 12.64 Principe des réseaux virtuels.

Les réseaux virtuels permettent de réaliser des réseaux axés sur l'organisation de l'entreprise tout en s'affranchissant de certaines contraintes techniques, notamment celles liées à la locali-

© Dunod – La photocopie non autorisée est un délit

sation géographique des équipements. En définissant des domaines de diffusion (domaine de broadcast) indépendamment de la situation géographique des systèmes, les VLAN autorisent une répartition et un partage optimal des ressources de l'entreprise.

Les VLAN introduisent la notion de segmentation virtuelle, qui permet de constituer des sous-réseaux logiques selon des critères prédéfinis (ports, adresses MAC ou réseau...). Un logiciel d'administration permet d'affecter chaque système raccordé au commutateur à un réseau logique d'appartenance. L'affectation peut être introduite manuellement par l'administrateur station par station (affectation statique) ou automatiquement (affectation dynamique). Chaque VLAN défini est ainsi à la fois un domaine de collision (technologie Ethernet), un domaine de broadcast (domaine de diffusion), un domaine de multicast (liaison logique point à multipoint) et un domaine d'unicast (liaison logique point à point). Ainsi, un broadcast émis par une station n'est diffusé que vers les stations appartenant au même VLAN.

La figure 12.64 illustre la réalisation de deux VLAN autour d'un même commutateur. L'administrateur a défini la configuration et généré la table des VLAN. Chaque VLAN constitue un domaine de communication. Ainsi la station connectée au port A du commutateur ne peut communiquer qu'avec les stations raccordées aux ports B et C. La figure 12.64 illustre une communication entre les stations raccordées aux ports A et C. Dans le même temps, la station raccordée au port D émet un broadcast. Ce message de diffusion ne sera répété que sur les ports appartenant au même VLAN que le port D, soit E et F.

12.8.2 Les différents niveaux de VLAN

Les échanges à l'intérieur d'un domaine sont sécurisés et les communications interdomaines sont autorisées et peuvent être contrôlées (autorisation ou interdiction de communiquer avec une ou plusieurs stations d'un autre domaine). L'appartenance à un VLAN étant définie logiquement et non géographiquement, les VLAN permettent d'assurer la mobilité (déplacement) des postes de travail. Selon le regroupement effectué, on distingue :

– les VLAN de niveau 1 ou VLAN par port (*Port-Based* VLAN) : ces VLAN regroupent des stations connectées à un même port du commutateur. La configuration est statique, le déplacement d'une station implique son changement de VLAN. C'est le mode le plus sécurisé, un utilisateur ne peut changer sa machine de VLAN. Un port, donc les stations qui lui sont raccordées, peut appartenir à plusieurs VLAN ;

– les VLAN de niveau 2 ou VLAN MAC (*MAC Address-Based VLAN*) : ces VLAN associent les stations par leur adresse MAC. De ce fait, deux stations raccordées à un même port (segment) peuvent appartenir à deux VLAN différents. Les tables d'adresses sont introduites par l'administrateur. Il existe des mécanismes d'apprentissage automatique d'adresses, l'administrateur n'ayant plus qu'à effectuer les regroupements par simple déplacement et regroupement de stations dans le logiciel d'administration (*Drag& Drop*). Une station peut appartenir à plusieurs VLAN. Les VLAN de niveau 2 sont indépendants des protocoles supérieurs. La commutation, s'effectuant au niveau MAC, autorise un faible temps de latence (commutation très efficace) ;

– les VLAN de niveau 3 ou VLAN d'adresses réseaux (*Network Address-Based VLAN*) : ces VLAN sont constitués de stations définies par leur adresse réseau (plage d'adresses) ou par masque de sous-réseau (subnet d'IP). Les utilisateurs d'un VLAN de niveau 3 sont affectés dynamiquement à un VLAN. Une station peut appartenir à plusieurs VLAN par

affectation statique. Ce mode de fonctionnement est le moins performant, le commutateur devant accéder à l'adresse de niveau 3 pour définir le VLAN d'appartenance. L'adresse de niveau 3 est utilisée comme étiquette, il s'agit bien de commutation et non de routage. L'en-tête n'est pas modifié.

Il est aussi envisageable de réaliser des VLAN par :

– protocole (IP, IPX...), la communication ne pouvant s'établir qu'entre stations utilisant le même protocole ;

– par application (N° de port TCP), la constitution des VLAN est alors dynamique, un utilisateur pouvant successivement appartenir à des VLAN différents selon l'application qu'il utilise ;

– par mot de passe (constitution dynamique des VLAN au login de l'utilisateur).

La figure 12.65 illustre ces différentes approches. Les VLAN peuvent être définis sur un ou plusieurs commutateurs, que ceux-ci soient locaux ou distants. Cependant, il devra y avoir autant de liens intercommutateurs (physiques ou virtuels) que de VLAN interconnectés.

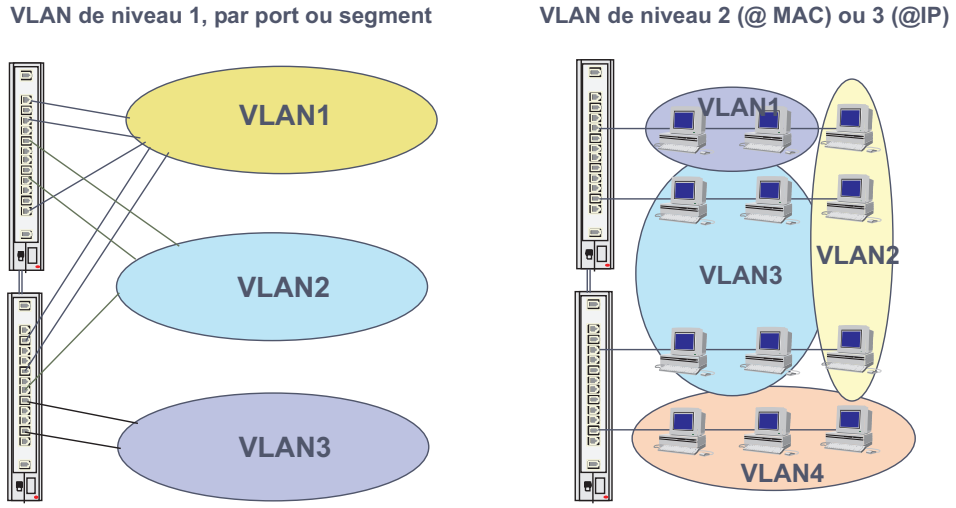


Figure 12.65 Les différents niveaux de VLAN.

12.8.3 L'identification des VLAN (802.1Q)

Principe

Lorsqu'un réseau comporte plusieurs commutateurs, chaque commutateur doit pouvoir localiser toutes les machines (table d'acheminement) et connaître le VLAN d'appartenance de la source et du destinataire (filtrage de trafic). Lorsque le réseau est important les tables peuvent devenir très grandes et pénaliser les performances. Il est plus efficace d'étiqueter les trames (figure 12.66). L'étiquette identifie le VLAN de la station source, le commutateur n'a plus alors qu'à connaître les VLAN d'appartenance des stations qui lui sont raccordées. La norme IEEE 802.1Q définit l'étiquetage des trames.

© Dunod – La photocopie non autorisée est un délit

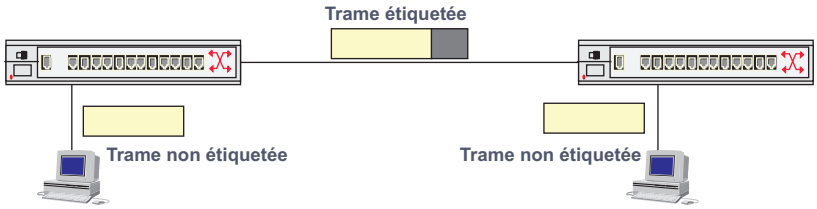


Figure 12.66 Principe de l'étiquetage des trames dans les VLAN.

La norme IEEE 802.1p/Q

Un VLAN correspond à un domaine de broadcast. Cependant, lorsque plusieurs VLAN sont définis sur un même segment cette définition est mise en défaut. Il est évidemment possible d'imaginer que le commutateur transforme le broadcast en une rafale d'unicasts. La solution adoptée par l'IEEE est toute différente : un seul VLAN peut être déclaré par port, les VLAN sont définis dans les normes 802.1Q et 802.1p (802.1p/Q[12]) qui introduisent quatre octets supplémentaires dans la trame MAC afin d'identifier les VLAN (*VLAN tagging*) et de gérer 8 niveaux de priorité (*Qualité of Service*, QoS). La figure 12.67 illustre l'étiquetage d'une trame MAC des réseaux de type 802.3.

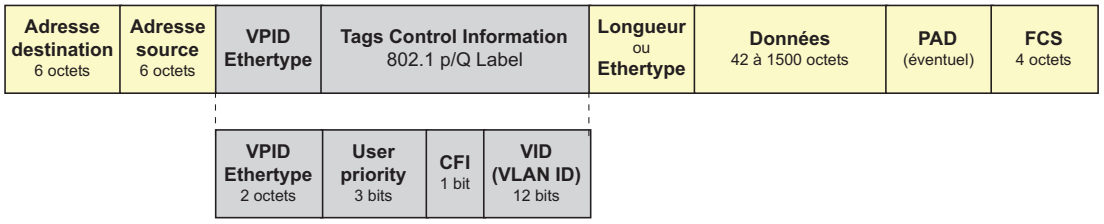


Figure 12.67 Format de la trame 802.1p/Q.

La trame 802.1p/Q augmente la taille de la trame 802.3. La taille maximale passe de 1 518 à 1 522 octets. Ce format limite l'usage de la trame en interne au commutateur et au dialogue intercommutateur (figure 12.68).

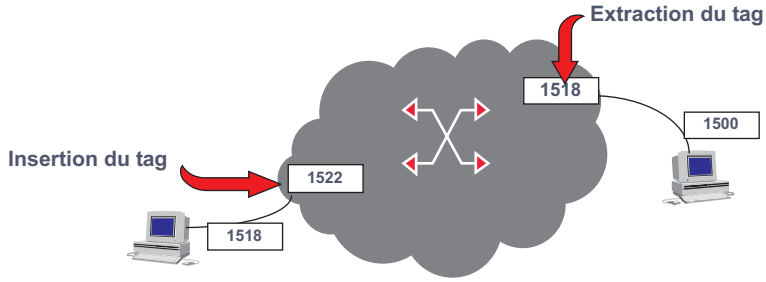


Figure 12.68 Identification des VLAN interne au réseau.

Pour garantir la compatibilité avec l'existant, le marquage des trames est vu comme une encapsulation supplémentaire. Ainsi, le champ **VPID** (*VLAN Protocol ID*) est similaire au

12. 802.1Q concerne les VLAN, 802.1p concerne la qualité de service.

champ Ethertype de la trame 802.3, il identifie le format 802.1 p/Q, sa valeur est fixée à 0x8100. Les deux octets suivants permettent de définir huit niveaux de priorité (*User Priority*). Les commutateurs de dernière génération disposent de plusieurs files d'attente les trames sont affectées à telle ou telle file suivant leur niveau de priorité.

Le bit **CFI** (*Canonical Format Identifier*) est, en principe, inutilisé dans les réseaux 802.3, il doit être mis à 0. Dans les réseaux Token Ring, à 1, il indique que les données du champ routage par la source sont au format non canonique. Le champ **VID** (*VLAN IDentifier*) identifie sur douze bits le VLAN destination. L'introduction de quatre octets supplémentaires implique que les commutateurs d'entrée et de sortie recalculent le FCS. On commence à trouver des cartes transporteurs capables de supporter le tagging.

12.9 LES RÉSEAUX SANS FIL

12.9.1 Généralités

S'affranchissant d'une infrastructure câblée et autorisant la mobilité, les réseaux sans fils, sous des appellations génériques différentes, sont en plein essor. On distingue :

– les **WPAN** (*Wireless Personal Network*), de la simple liaison infrarouge à 100 kbit/s au Bluetooth à environ 1 Mbit/s, ces technologies peu coûteuses devraient se développer rapidement. Elles sont essentiellement utilisées pour raccorder un périphérique informatique (imprimante...), un agenda électronique...

– les **WLAN** (*Wireless Local Area Network*), prolongent ou remplacent un réseau local traditionnel. Ces réseaux, objet de ce paragraphe, devraient connaître un développement important. Ils autorisent des débits allant de 2 à 54 Mbit/s ;

– les **WMAN** (*Wireless Metropolitain Area Network*) utilisés pour l'accès aux réseaux d'infrastructure (boucle locale), ils offrent des débits de plusieurs dizaines de Mbit/s ;

– enfin, les **WWAN** (*Wireless Wide Area Network*), recouvrent essentiellement les réseaux voix avec ses extensions données (GSM, GPRS et UMTS), les débits sont relativement faibles de quelques dizaines de kbit/s (10 à 384 kbit/s).

Le tableau de la figure 12.69 présente une synthèse des principales technologies.

Nom	Fréquence	Débit	Portée	Commentaires
Bluetooth	2,4 GHz	1 à 10 Mbit/s	10-100 m	Utilisation personnelle
Wi-Fi (802.11b)	2,4 GHz	11 Mbit/s	300 m	Liaison point à point à haut débit
Home RF	2,4 GHz	1,6 et 10 Mbit/s	50 m	Domotique
IEEE 802.11g	2,4 GHz	54 Mbit/s		Successeur du 802.11b
IEEE 802.11a	5 GHz	54 Mbit/s		Idem.
HiperLan 2	5 GHz	54 Mbit/s		Concurrent du 802.11a

Figure 12.69 Les principales solutions de réseaux sans fil.

© Dunod – La photocopie non autorisée est un délit

12.9.2 Architecture générale des réseaux sans fil

Les réseaux « ad hoc »

Les réseaux « ad hoc » s'affranchissent de toute infrastructure. La communication à lieu directement de machine à machine. Une machine pouvant éventuellement servir de relais pour diffuser un message vers une station non vue (au sens électromagnétique du terme) par la station d'origine (routage).

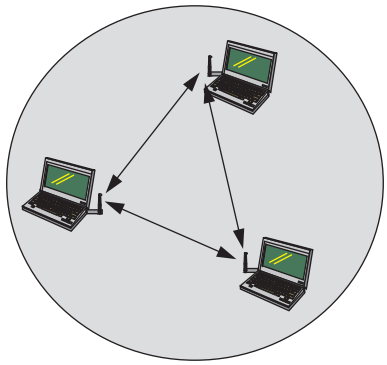


Figure 12.70 Microcellule ad hoc.

Actuellement, les réseaux ad hoc ne fonctionnent qu'en mode point à point. Les protocoles de routage font l'objet de nombreuses recherches. Le principe[13] du routage reste cependant identique, lorsqu'une station veut en joindre une autre elle inonde le réseau, son message est répété par toutes les stations jusqu'à la station destination. Le destinataire acquitte le premier message reçu qui emprunte en retour la même voie qu'à l'aller. Chaque machine apprend ainsi la route pour joindre le destinataire (la route est construite à l'envers).

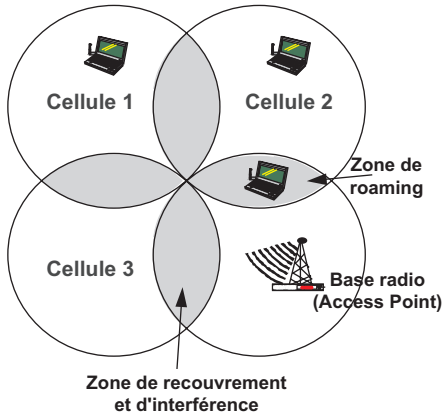


Figure 12.71 Principe d'un réseau cellulaire.

13. Ces techniques posent aujourd'hui de nombreux problèmes, en relation avec la sécurité (les messages sont stockées par les stations avant réémission) et la fiabilité (arrêt d'une station en cours de retransmission...).

Les réseaux cellulaires

Les réseaux sans fils sont soit indépendants de toute infrastructure filaire, soit en prolongement de celle-ci. Les solutions adoptées doivent résoudre de nombreux problèmes :

– la bidirectionnalité de la communication ainsi que le nombre de communications à établir en même temps pose le problème de l'allocation de fréquences. Le partage du spectre a introduit la notion de communication cellulaire. Une cellule est une zone dans laquelle les fréquences utilisées appartiennent à un même ensemble. Deux cellules adjacentes ne devront pas utiliser le même ensemble de fréquences (figure 12.71) ;

– l'accès multiple et le partage du support (politique d'accès) ;

– la localisation du mobile en déplacement (itinérance ou *roaming*) ;

– la possibilité pour le mobile en déplacement de maintenir la communication en cours (*hand over* ou *handoff*) ;

– l'identification et la confidentialité des communications.

Une cellule est centrée autour de sa base radio (**AP**, *Access Point*). Lorsqu'un mobile quitte une cellule (**BSS**, *Basic Service Set*), pour maintenir la communication, il doit être accueilli par une autre cellule. Les techniques de gestion de la mobilité sont différentes selon que le mobile est un mobile voix (téléphone) ou un mobile données (station). Une communication téléphonique peut être interrompue quelques millisecondes sans nuire à l'intelligibilité de la conversation (temps de basculement d'une cellule vers une autre). Dans un service données, la moindre interruption provoque une erreur de transmission. Dans ces conditions, le basculement d'une cellule ne peut avoir lieu que dans la zone de recouvrement des cellules et en fin de transmission d'un paquet, on parle alors seulement de *roaming* et non plus de *hand over* (figure 12.71).

12.9.3 Les réseaux 802.11

Architecture

Le réseau IEEE 802.11 est basé sur une architecture de type cellulaire (figure 12.72).

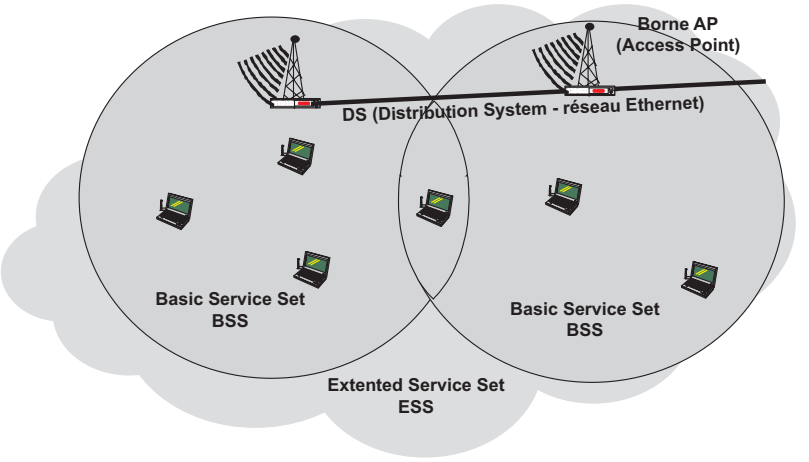


Figure 12.72 Architecture matérielle du réseau IEEE 802.11.

© Dunod – La photocopie non autorisée est un délit

Chaque cellule, **BSS** (*Basic Service Set*), est contrôlée par une base radio, (**AP**, *Access Point*). Le réseau peut comporter une ou plusieurs cellules autonomes ou être le prolongement d'un réseau Ethernet traditionnel. Dans ce dernier cas, les différents points d'accès sont reliés à un réseau de distribution qui fait office de backbone (**DS**, *Distribution System*). L'ensemble forme un seul réseau 802 désigné sous le terme de **ESS** (*Extended Service Set*). Les réseaux 802.3 et 802.11 sont interconnectés par un élément actif assurant l'adaptation des formats : le portail.

L'accès au support

➤ Notion de station cachée

À l'instar d'Ethernet, les stations d'un réseau sans fil se partagent le même média. Le protocole CSMA utilisé dans les réseaux Ethernet n'est pas applicable tel quel. La figure 12.73 illustre ce fait. La station A doit transmettre des données à destination de la station B. Elle écoute le support, celui-ci est libre, elle émet. Cependant, dans le même temps, la station C désire aussi transmettre des données à B ou à une autre machine de la zone d'interférence. La station C est hors de portée de A (station cachée), elle n'entend pas le message de A, et considère le support libre, elle transmet ses données. Les données de A et de C sont polluées, il y a collision.

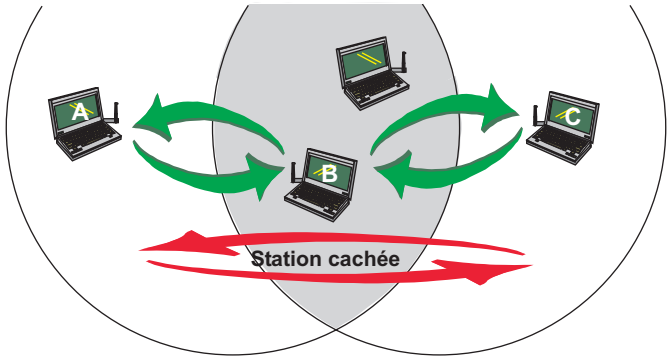


Figure 12.73 Problème de la station cachée.

➤ Le CSMA/CA

L'algorithme d'accès ou **DCF** (*Distributed Coordination Function*) est une version adaptée du CSMA, le **CSMA/CA** (*Carrier Send Multiple Access with Collision Avoidance*, signifiant à prévention de collision). Détecter une collision nécessite une transmission de type *full duplex*, or, en environnement radio, la puissance d'émission éblouirait le récepteur, cette approche est irréalisable à coût raisonnable. Il est donc impératif d'implémenter un mécanisme qui rend la probabilité de collision aussi faible que possible c'est l'objet du CSMA/CA dont le principe est illustré en figure 12.74. Un mécanisme d'accusé de réception complète le système.

Une station qui veut émettre écoute le support (CSMA). Si le support est occupé, elle diffère son émission. Si le support est libre, elle émet un petit paquet (**RTS**, *Request To Send*) qui contient les adresses source et destination ainsi qu'une durée correspondant au temps d'émission des données et au délai d'acquittement (réservation d'une tranche canal). Si le support est libre, la station destination répond (**CTS**, *Clear To Send*), le message comporte les mêmes

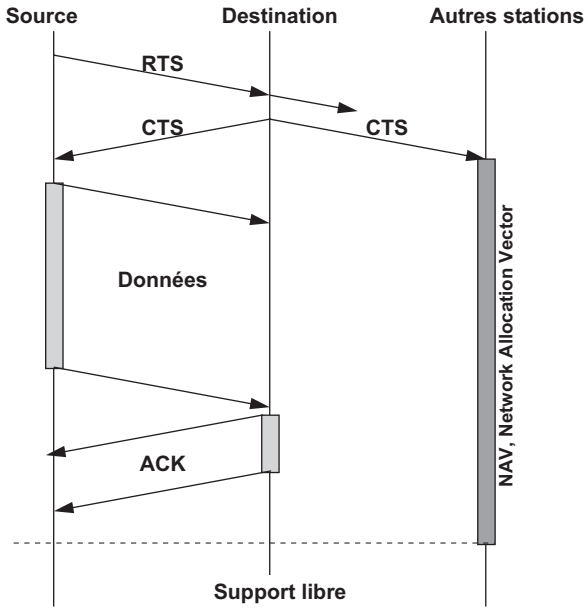


Figure 12.74 Méthode d'accès au support.

informations que le RTS. Ainsi, la station C (station cachée de A) de la figure 12.73 qui n'a pas reçu le message de A, reçoit celui de B qui comporte les mêmes informations, elle est donc informée de la demande de réservation de bande formulée par A. Toutes les stations recevant le RTS ou le CTS arment une temporisation (*Virtual Carrier Sense*) correspondant au temps de réservation demandé (**NAV**, *Network Allocation Vector*).

La probabilité de collision est d'autant plus faible que le message est court. À cet effet, la norme IEEE 802.11 introduit la segmentation au niveau MAC.

12.10 ASPECT PROTOCOLAIRE

12.10.1 Généralités

Indépendamment des systèmes d'exploitation réseau (**NOS**, *Network Operating System*), les performances générales et les possibilités d'interconnexion des réseaux sont directement liées à la pile de protocoles utilisée. Les principaux protocoles mis en œuvre dans les réseaux locaux sont symbolisés figure 12.75.

12.10.2 Les piles ISO

Seuls, les réseaux de type industriel (MAP et TOP) ont implémenté une pile ISO. Le réseau **MAP** (*Manufactoring Automation Protocol*), d'origine General Motors est entièrement orienté vers les processus industriels, il repose sur un réseau bus à jeton (802.4). Le réseau **TOP** (*Tech-*

© Dunod – La photocopie non autorisée est un délit

nical and Office Protocol), d'origine Boeing, prend en compte les besoins bureautiques, il s'appuie sur des couches MAC 802.4, 802.3 et 802.5. La figure 12.76 présente ces architectures.

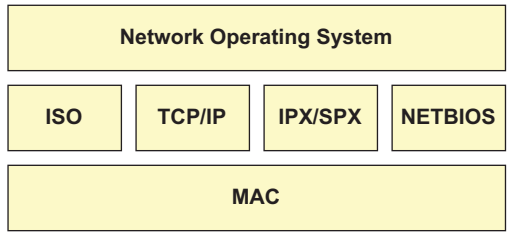


Figure 12.75 Les principales piles de protocoles utilisées dans les LAN.

De manière générale, les piles ISO utilisent TP4 et **CLNP** (*ConnectionLess Network Protocol*, ISO 8473). L'adressage résulte de la concaténation d'une adresse X.121 (*Net_Id*) et de l'adresse MAC (*Host_Id*).

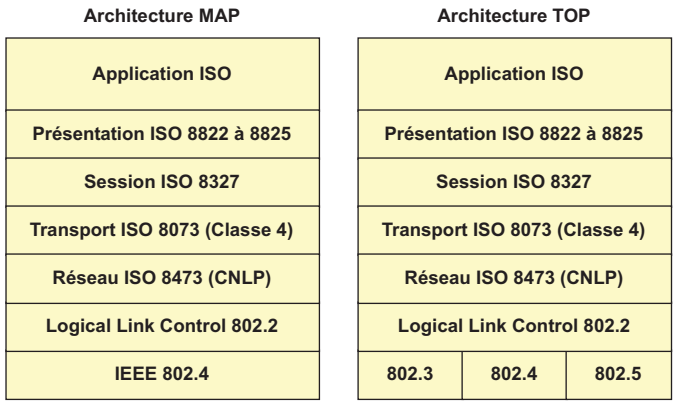


Figure 12.76 Les réseaux MAP et TOP.

12.10.3 La pile IPX/SPX

Présentation

En voie de disparition, mais encore présente dans de nombreux réseaux, la pile **IPX/SPX** (*Internet Packet eXchange/Sequenced Packet eXchange*) est une adaptation par Novell de l'architecture **XNS** (*Xerox Network System*) de Xerox. La similitude des deux architectures représentées figure 12.77 est très apparente.

Le protocole *Echo* sert à vérifier l'existence d'une route pour atteindre une station (Ping de TCP/IP). Le protocole *Error* sert à signaler à l'émetteur d'un paquet une erreur sur celui-ci (ICMP de TCP/IP). Le protocole SPX (**SPP**, *Sequenced Packet Protocol de XNS*) assure un service de transport en mode connecté (TCP de TCP/IP). Le protocole **PEP** (*Packet Exchange Protocol*) est un service de transport en mode non connecté, cependant celui-ci est capable d'effectuer une reprise sur erreur. Le protocole **RIP** (*Routing Information Protocol*) achemine les paquets à travers un réseau (protocole de routage).

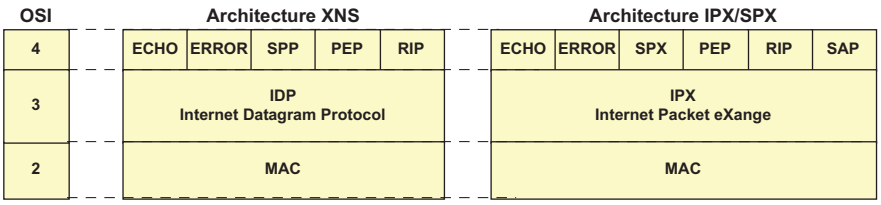


Figure 12.77 Comparaison des architectures XNS et IPX/SPX.

Sur les serveurs, le protocole **SAP** (*Service Advertisement Protocol*) informe, à intervalle régulier, les stations connectées au réseau des différents services disponibles (partage de fichiers, imprimantes, service de synchronisation d'horloge...). Le service SAP utilise des broadcasts, pour permettre les annonces sur tout le réseau, les routeurs ont dû être adaptés pour transmettre ces broadcasts.

Le protocole IPX

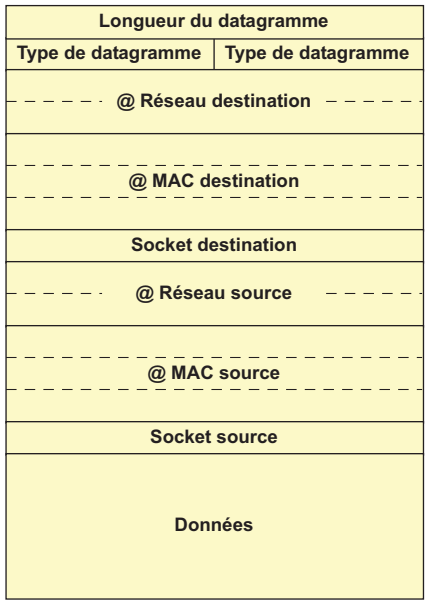


Figure 12.78 Datagramme IPX.

Le protocole **IPX** (*Internet Protocol eXchange*), amélioration du protocole IDP (*Internet Datagram Protocol*) de XNS, offre un service de niveau 3 en mode datagramme (IP de TCP/IP). Les services d'IPX sont accessibles directement ou via les protocoles de niveaux supérieurs (PEP, SPX) et **NCP** (*Netware Core Protocol*).

Afin de conserver une certaine compatibilité avec XNS, la structure du paquet IPX est similaire à celle de IDP. La figure 12.78 représente le datagramme IPX.

Le champ total de contrôle n'est conservé que pour la compatibilité avec XNS, il est initialisé à 0xFFFF. Le champ longueur datagramme indique la longueur totale du paquet, en-tête compris. La taille d'un datagramme IPX est limitée par le support MAC. L'indication temps de vie, initialisée à zéro est incrémentée d'une unité par chaque routeur traversé. Quand la valeur

© Dunod – La photocopie non autorisée est un délit

atteint 16, le paquet est détruit. Le champ type de datagramme précise le protocole encapsulé (00 type inconnu, 01 RIP...). Suivent les champs d'adressage.

Adressage IPX

Le datagramme IPX contient toutes les données nécessaires à l'adressage complet des données. Le champ adresse réseau permet de déterminer le réseau sur lequel est située la machine (Net_ID). Cette information est complétée par l'indication de l'adresse MAC de la station. Le fait d'avoir choisi comme Host_ID l'adresse physique du coupleur garantit l'unicité d'adresse et simplifie la tâche de l'administrateur de réseau lors de la configuration. Cette approche a été reprise dans IPv6 (EUI-64).

La notion d'unicité d'adressage réseau est absente dans IPX, il n'y a pas d'organisme international de gestion de l'espace d'adressage. Celle de plan d'adressage est très réduite, et peut poser quelques problèmes lors de l'interconnexion de plusieurs réseaux. L'adresse réseau zéro indique le réseau sur lequel on est. De ce fait, si le réseau n'est interconnecté à aucun autre, ce champ n'a pas besoin d'être renseigné. Ces informations sont complétées par l'indication du *socket*, notion équivalente à celle de port TCP/IP ou à celle T_SAP d'ISO.

12.10.4 La pile NETBIOS

Présentation

NetBIOS (*Network Basic Input/Output System*) est un ensemble de protocoles réseaux. Non conforme au modèle de référence, NetBios a été développé par la société Sytek pour le réseau IBM PC NetWork. Adopté par Microsoft, NetBios devint vite, malgré ses faiblesses, un standard du marché. La pile NetBios est représentée figure 12.79.

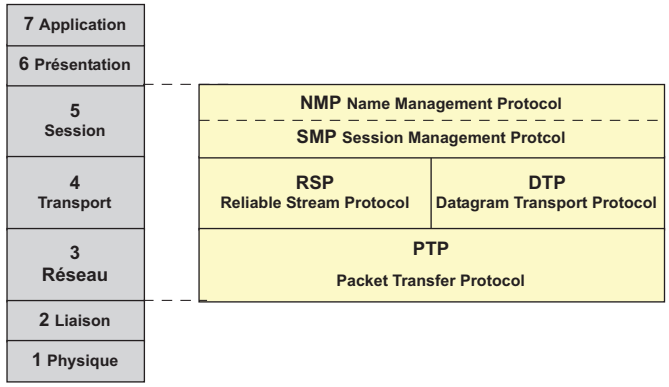


Figure 12.79 L'architecture NetBIOS.

NetBios couvre les couches 3 à 5 du modèle de référence. La couche 3, **PTP** (*Packet Transfer Protocol*) implémente un service de datagramme. Il n'y a pas, dans NetBIOS, de notion d'adressage réseau. Prévu initialement pour de petits réseaux, NetBIOS n'utilise que l'adresse MAC. Le service transport offre les deux types de service, un service en mode non connecté (**DTP**, *Datagram Transport Protocol*), et un service en mode connecté (**RSP**, *Reliable Stream Protocol*). RSP établit un circuit entre les deux participants à l'échange, il offre un service

complet de contrôle et reprise sur erreur, contrôle de séquencement. Le protocole **SMP** (*Session Management Protocol*) est un service de session, il établit une session entre les deux entités, cette session est ouverte lors d'une phase de connexion et est fermée lors d'une phase de déconnexion. Des échanges hors session restent possibles.

Notion de service de noms

NetBIOS n'ayant pas, au début du moins, vocation à être implémenté sur de vastes réseaux, il n'utilise pas d'adresse réseau, NetBIOS identifie tous les objets réseaux par un nom simple (15 caractères alphanumériques et le 16e caractère précise le type d'objet nommé). Le protocole **NMP** (*Name Management Protocol*) réalise la correspondance entre le nom NetBIOS (connu de l'utilisateur) et l'adresse MAC (non connue de l'utilisateur). La figure 12.80 compare la résolution de noms sous IP et sous NetBIOS.

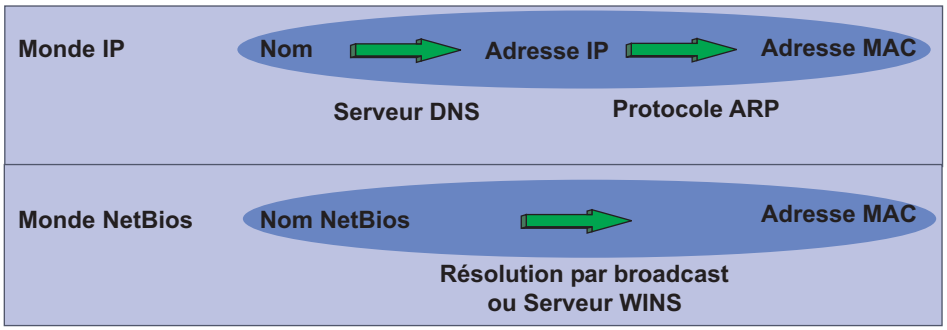


Figure 12.80 Résolution de noms sous NetBios.

Une machine qui se raccorde au réseau commence par diffuser son nom. Toutes les stations connectées apprennent ainsi le nom et l'adresse MAC de la station. Les différents couples Nom/MAC sont mémorisés (cache NetBIOS). Lorsqu'un utilisateur veut joindre une station, il fournit son nom, si ce nom n'est pas dans la table locale des noms, le protocole NMP diffuse une requête sur le réseau, seule la station qui reconnaît son nom répond, diffusant ainsi son nom et son adresse MAC à l'ensemble du réseau. N'utilisant pas d'adresse réseau, NetBIOS n'est pas routable.

Évolution de NetBIOS, l'émulation NetBIOS

NetBIOS se présentait, pour les programmeurs, comme une interface de programmation réseau de haut niveau. Il définit une structure de données (**NCB**, *Network Control Block*) et 18 fonctions qui suffisent à toutes les actions sur le réseau. De nombreux programmeurs utilisent les services NetBIOS. De ce fait, tous les environnements réseaux sont capables d'émuler NetBIOS.

Pour améliorer les performances et conserver les fonctionnalités de NetBIOS (service de noms et gestion des sessions), l'environnement primitif a été scindé en deux :

– la couche NetBIOS qui gère les sessions et le service de noms ;

– la couche **NetBEUI** (*Network Bios Extended User Interface*) qui assure les fonctions de transport.

© Dunod – La photocopie non autorisée est un délit

La figure 12.81 représente les différents environnements NetBIOS.

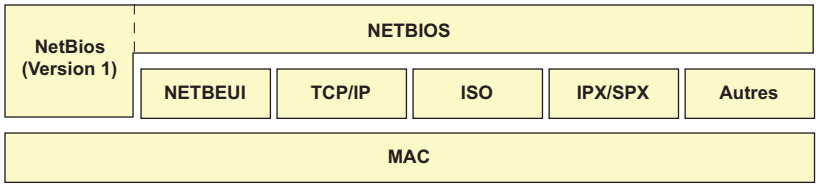


Figure 12.81 Émulation NetBIOS sur les différentes architectures.

12.11 LES CANAUX HAUTS DÉBITS

D'abord définis comme de simples interfaces haut débit entre calculateurs et périphériques, les canaux hauts débits se sont, avec l'introduction de commutateurs qui ont autorisé les relations multiples entre périphériques à haut débit ou stations de travail, rapprochés des réseaux de diffusion. Les principales solutions d'interconnexion de cette catégorie sont les interfaces **HiPPI** et **Fibre Channel**.

12.11.1 HiPPI

L'interface **HiPPI** (*High Performance Parallel Interface*), normalisée par l'ANSI (ANSI X3.183, X3.222), est un canal de transmission haut débit (800 Mbit/s) entre un calculateur et ses périphériques. HiPPI définit un mode de transmission unidirectionnelle en parallèle sur un support cuivre (paires torsadées, 1 paire par bit) en mode connecté. Deux interfaces HiPPI sont nécessaires pour réaliser une communication *full duplex*. L'interface d'origine (800 Mbit/s) utilise un câble 50 paires dont 32 pour la transmission de données (mot de 32 bits), les paires restantes (18 bits) servent à la signalisation (figure 12.82), la distance maximale est de 25 m. Un débit de 1,6 Gbit/s peut être obtenu par l'utilisation simultanée de deux câbles de 50 paires (mots de 64 bits).

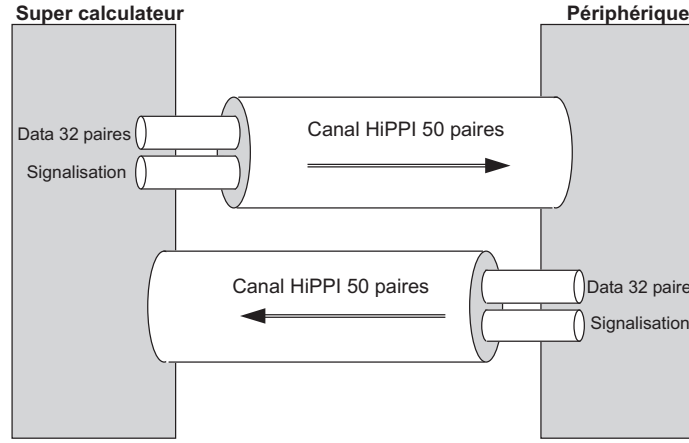


Figure 12.82 Principe des canaux HiPPI.

La transmission se fait en mode paquets par rafale. HiPPI fournit les mécanismes nécessaires au contrôle d'erreur (bit de parité), contrôle de flux et à l'adressage des différents périphériques. L'efficacité de la synchronisation est garantie par un codage des signaux du type 20B/24B. L'introduction d'un commutateur de type crossbar (HiPPI-SC, *Crossbar Switch*) a permis le partage d'un même canal par plusieurs périphériques ou calculateurs, une seule interface est alors nécessaire pour chaque élément raccordé au réseau HiPPI ainsi formé.

Compte tenu de la limitation à 25 m, une interface optique a été définie (*Serial HiPPI*) dont la portée est alors de 1 km pour la fibre multimode et de 10 km pour la fibre monomode.

12.11.2 Fibre Channel Standard

Évolution des canaux sur fibre optique, **FCS** (*Fibre Channel Standard*) définit une interconnexion à haut débit en mode série autour d'un commutateur spécifique appelé la « *Fabric* » (figure 12.83).

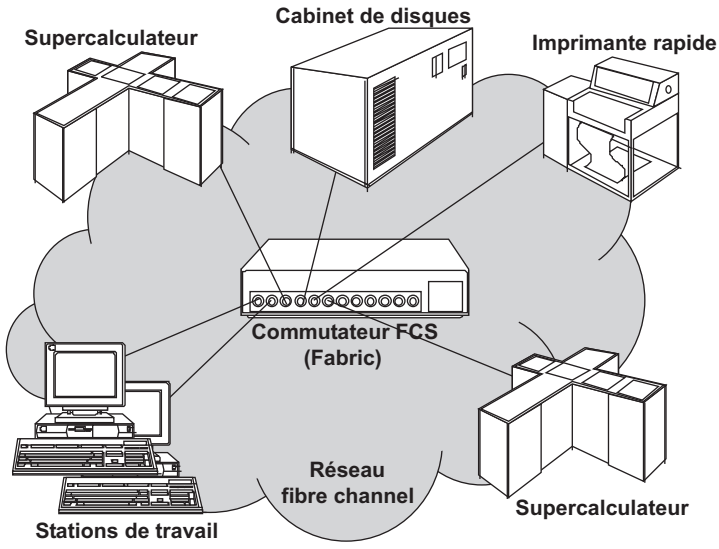


Figure 12.83 Principe du FCS (*Fibre Channel Standard*).

Le commutateur principal (*Fabric*) assure les fonctions de routage (adressage sur 24 bits du type hiérarchique), de contrôle d'erreur et de contrôle de flux. Il supporte les protocoles de haut niveau comme IP (*Internet Protocol*), les interfaces IPI (*Intelligent Peripherical Interface 3*), SCSI (*Small Computer System Interface*) et HiPPI. L'architecture du commutateur est structurée en cinq couches (figure 12.84) :

– la couche FC-0 assure l'adaptation au support en fonction de la classe de débit offerte (133 à 1 062 Mbit/s),
– la couche FC-1 définit le protocole de transmission et les règles de codage (8B/10B),
– la couche FC-2 détermine la structure de trame, la signalisation et définit, à l'instar de LLC (*Logical Link Control*), trois types de services : le mode orienté connexion (mode circuit virtuel ou classe 1), le mode sans connexion mais avec acquittement (classe 2) et le mode sans connexion et sans acquittement (mode datagramme ou classe 3),

© Dunod – La photocopie non autorisée est un délit

– la couche FC-3 définit un ensemble de services, notamment le mode diffusé (*multicasting*) par regroupement de ports,
– enfin la couche FC-4 assure l'adaptation de FCS (*Fibre Channel Standard*) aux protocoles supérieurs.

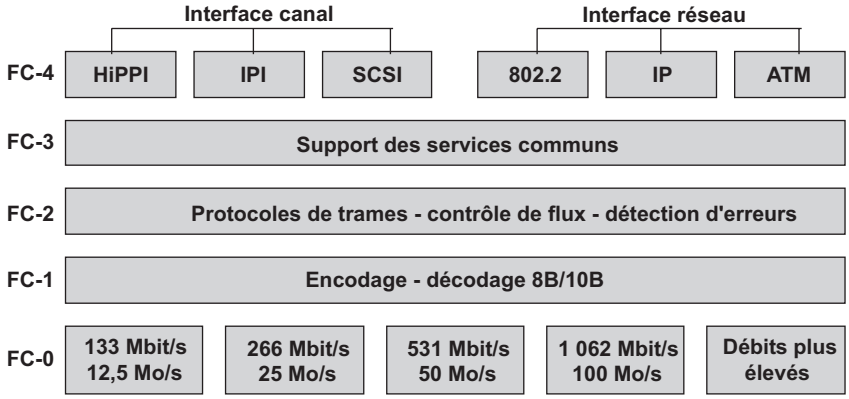


Figure 12.84 Architecture de FCS (*Fibre Channel Standard*).

12.12 CONCLUSION

Les réseaux locaux constituent aujourd'hui le moyen d'accès aux systèmes d'information le plus utilisé. Pour surmonter leur limitation en distances, en nombre de machines et en débit, les techniques des LAN ont été appliquées à des réseaux fédérateurs. Ces réseaux couramment appelés **MAN** (*Metropolitain Area Network*) sont étudiés dans le chapitre suivant.

EXERCICES

Exercice 12.1 Distinction IEEE 802.3 et Ethernet

Comment peut-on distinguer un réseau Ethernet d'un réseau IEEE 802.3 ?

Exercice 12.2 Adressage MAC, type d'adresse

a) Quel est le format de l'adresse MAC et la signification de chacun des 4 champs.

b) Quels sont les types d'adresse MAC auxquels une station doit répondre ?

c) A quel type d'adresse correspond l'adresse MAC 01-00-5E-AB-CD-EF, cette adresse peut-elle être présente dans le champ adresse source ?

d) Déduisez-en un type d'application possible.

Exercice 12.3 Notation canonique et non canonique

Écrivez l'adresse MAC de broadcast généralisé en notation canonique et non canonique

Exercice 12.4 Comparaison des topologies et méthodes d'accès

Établissez un tableau comparatif (avantages, inconvénients) des différentes topologies et des différentes méthodes d'accès utilisées dans les réseaux locaux.

Exercice 12.5 Synchronisation des réseaux

Une séquence de synchronisation bit de 7 octets en 802.3 précède le délimiteur de début de trame, ce n'est pas le cas en 802.5. Justifiez ce choix.

Exercice 12.6 Rapidité de modulation

Quelle est la rapidité de modulation en bauds d'un réseau local 802.3 (Ethernet) lorsqu'il émet une suite continue de 1 ou de 0 ?

Exercice 12.7 Longueur de l'anneau

Quelle est l'influence sur la longueur virtuelle de l'anneau à jeton (802.5) de l'insertion d'une nouvelle station si le coefficient de vélocité du câble utilisé est de 2/3 ?

Exercice 12.8 Conception d'un réseau

On veut concevoir un réseau local sur fibre optique, le cahier des charges spécifie :

– longueur maximum du support physique 200 km ;

– nombre maximum de stations connectées 1 000 ;

© Dunod – La photocopie non autorisée est un délit

– vitesse de propagation sur le support 200 000 km/s ;
– débit binaire nominal 100 Mbit/s ;
– longueur maximum d'une trame : 4 500 octets ;
– implémentation du protocole CSMA/CD.

Qu'en pensez-vous ?

Exercice 12.9 Efficacité du protocole 802.5

Compte tenu des résultats de l'exercice précédent, les concepteurs imaginent utiliser le protocole 802.5. Quel sera alors le débit maximum d'information ?

Exercice 12.10 Détermination du temps d'accès

Un réseau 802.5 à 4 Mbit/s comporte 50 stations, la distance moyenne entre stations est de 50 m. La vitesse de propagation étant de 200 m/μs, on demande :

– Quel est le temps maximum au bout duquel une station est assurée de disposer du jeton ?
– Quel est, dans cette situation, le débit du réseau, vu d'une station ?
– Peut-on effectuer un calcul similaire pour les réseaux CSMA/CD ?

Exercice 12.11 Commutateur ou hub ?

Compléter le tableau de la figure 12.85 ci-dessous en indiquant quel équipement est le mieux adapté en fonction des performances et des applications.

Objectifs	Équipement recommandé
Réseaux données peu chargé, recherche de la performance	
Réseaux données très chargé, recherche de la performance	
Réseaux voix/données sur IP	

Figure 12.85 Équipement et objectifs.

Exercice 12.12 Plan d'adressage

Votre entreprise comporte 4 établissements : Paris, Strasbourg, Brest et Marseille reliés en étoile par des LL (liaisons louées). Compte tenu des informations ci-dessous, on vous demande d'établir le plan d'adressage de votre entreprise :

– les LL seront adressées en point à point ;
– chaque établissement devra pouvoir distinguer 10 sous-réseaux ;
– chaque sous-réseau pourra éventuellement comprendre plus de 500 machines mais moins de 1 000.

On devra pouvoir distinguer simplement l'établissement. N'ayant aucun besoin de connexion vers l'extérieur, l'entreprise utilisera des adresses privées de classe A.

Chapitre **13**

Les réseaux métropolitains FDDI, DQDB, ATM...

À l'origine, les réseaux métropolitains (**MAN**, *Metropolitan Area Network*) étaient essentiellement destinés à l'interconnexion de réseaux locaux d'entreprise. Fédérateurs de réseaux, ils offraient des débits élevés au regard du débit des composantes locales ($\geqslant$ 100 Mbit/s), et couvraient des distances importantes ($\geqslant$ 100 km). Devant le besoin croissant de débit, ils ont vite été utilisés en lieu et place des LAN traditionnels. Ces réseaux peuvent donc à la fois être considéré comme des réseaux locaux (LAN), s'ils sont utilisés essentiellement pour leur grand débit (100 Mbit/s ou plus) ou comme réseaux métropolitains s'ils le sont pour leurs caractéristiques de distance et les possibilités d'interconnexion de LAN.

Deux technologies ont longtemps dominé ce secteur : **FDDI** (*Fiber Distributed Data Interface*) et **DQBD** (*Distributed Queue Dual Bus*). N'offrant aucune qualité de service, ils n'ont pu rivaliser avec le développement de l'ATM jusqu'au poste de travail (LAN ATM). Ces techniques sont aujourd'hui très concurrencées par l'arrivée du Gigabit Ethernet dans les composantes locales et du 10 Gigabit Ethernet dans les boucles locales.

13.1 FDDI (FIBER DISTRIBUTED DATA INTERFACE)

13.1.1 Généralités

D'origine ANSI (ANSI X3T9.5), la technique FDDI a été normalisée par l'ISO (IS 9314). FDDI est un réseau en anneau optique sur fibre optique multimode. L'anneau est en fait un double anneau, ce qui permet une autocicatrisation du réseau en cas de défaillance d'un lien ou d'un nœud (figure 13.1). Le débit nominal est de 100 Mbit/s pour une distance maximale de 100 km (200 si l'on tient compte du double anneau). FDDI supporte jusqu'à 1 000 stations, distantes l'une de l'autre de moins de 2 km.

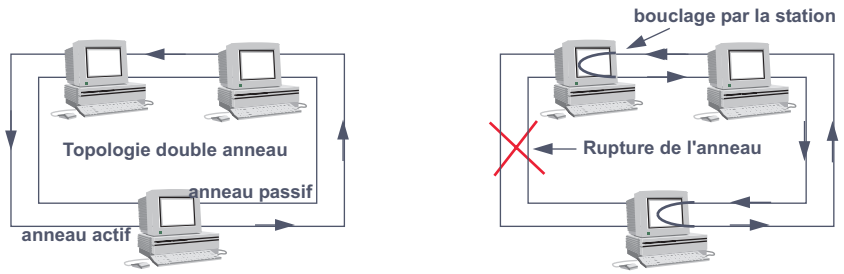


Figure 13.1 Reconfiguration rapide de l'anneau.

Une version de FDDI sur paire torsadée (**TPDDI**, *Twisted Pair Distributed Data Interface*) autorise des débits de 100 Mbits sur 100 m.

La méthode d'accès est similaire à celle du réseau IEEE 802.5 version 16 Mbit/s (**ETR**, *Early Token Release*). Pour accéder au support, une station doit posséder le jeton. Elle émet ses données et génère un nouveau jeton. Chaque station retire de l'anneau les données qu'elle y a déposées. Plusieurs trames de données, issues de stations différentes, peuvent circuler sur l'anneau, mais il n'y a qu'un seul jeton libre à la fois. Les différences essentielles, par rapport aux réseaux de type 802.5, sont :

– il n'y a pas de station monitrice, chaque station participe à la surveillance de l'anneau ;

– compte tenu de distance maximale interstation (2 km), de la longueur totale de l'anneau FDDI et du nombre de stations les dérives d'horloges peuvent être importantes. La synchronisation à partir d'une horloge unique n'est plus réalisable. Chaque station possède sa propre horloge (réseau plésiochrone). Une mémoire tampon (buffer élastique, **EB** *Elasticity Buffer*) permet de compenser les écarts entre l'horloge de réception et celle d'émission. C'est la capacité de la mémoire tampon mémoire qui limite la taille de la trame à 4 500 octets ; la figure 13.2 compare la distribution des horloges dans le cas d'un réseau synchrone et d'un réseau plésiochrone ;

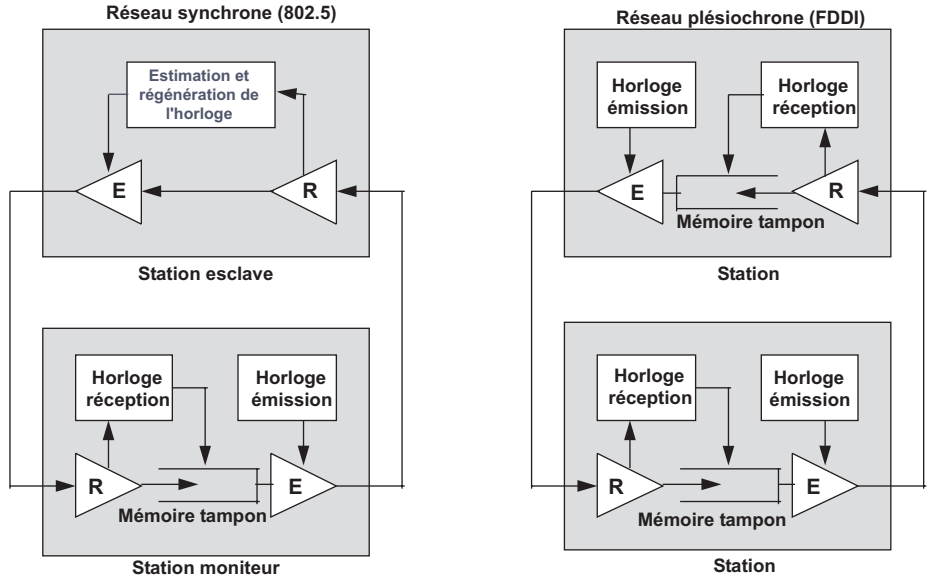


Figure 13.2 Distribution des horloges dans les réseaux en anneau.

– FDDI introduit une notion réduite de la qualité de service en définissant deux types de données : les données urgentes à contrainte de débit (classe synchrone) et les données sporadiques, sans contrainte particulière de débit (classe asynchrone). Lorsqu'une station possède le jeton, elle peut toujours émettre des données synchrones (données prioritaires) et, si et seulement si, le jeton est en avance (jeton temporisé), elle peut alors émettre des données asynchrones. L'émission de ces données correspond la récupération, par la station, de la bande non utilisée par les données de la classe synchrone.

L'indépendance des horloges émission et réception nécessite une phase de synchronisation avant l'interprétation des données reçues. En FDDI, cette phase est réalisée par un préambule de 6 à 8 octets (12 à 16 symboles *Idle*).

13.1.2 La méthode d'accès : le jeton temporisé

Les variables d'état

Pour garantir une certaine bande passante à chaque station, FDDI implémente une technique d'accès originale. Le jeton est dit temporisé, c'est-à-dire à l'initialisation de l'anneau une autonégociation détermine, en fonction des contraintes de chaque station, un temps maximal au bout duquel une station doit disposer du jeton (protocole déterministe), fixant ainsi pour garantir ce délai d'accès aux autres stations un temps maximal d'émission (données de la classe synchrone). Le mécanisme du jeton temporisé (*Timed Token Protocol*) est contrôlé par quatre variables d'état :

– **TTRT** (*Target Token Rotation Time*) : cette variable indique le temps maximal au bout duquel une station doit recevoir le jeton. La valeur de TTRT est négociée lors de l'initialisation de l'anneau. Chaque station propose, en fonction de ses contraintes de débit, une valeur maximale admissible de TTRT. C'est la plus faible valeur qui est retenue, elle correspond à celle de la station qui a les plus fortes contraintes de trafic. Chaque station a un temps d'émission défini (Ts), réservé à l'émission de données de la classe synchrone, tel que la somme de ces temps soit inférieure à TTRT (TTRT > [Ts · N] où N représente le nombre de stations actives).

– La variable **LC** (*Late_Counter*) autorise (LC = 0) ou interdit (LC = 1) l'émission de données de la classe asynchrone. Si le jeton arrive en avance (temps de rotation inférieur à TTRT), la variable LC est positionnée à zéro. Sinon, la valeur est positionnée à 1. Si le jeton arrive en retard alors que LC est déjà positionné à 1, la station provoque une réinitialisation de l'anneau.

– **TRT** (*Token Rotation Timer*) : ce timer est initialisé à la valeur de TTRT à chaque réception d'un jeton (si LC = 0), puis il décroît linéairement jusqu'à l'arrivée effective du jeton. Si le jeton arrive avant l'expiration du TRT et que la variable LC est égale à 0 à l'arrivée du jeton, la station peut émettre des données asynchrones pendant le temps restant (THT) et des données synchrones pendant le temps d'émission qui lui est imparti (Ts). Si le jeton arrive alors que TRT est nul, elle ne peut émettre que des données synchrones pendant le temps Ts. Attention, TRT ne mesure pas le temps de rotation du jeton, mais l'avance du jeton.

– **THT** (*Token Holding Timer*) : ce temporisateur mesure le temps d'émission de données de la classe asynchrone. Quand le jeton arrive en avance, THT est initialisé à TRT (avance du jeton), et TRT est réinitialisé à TTRT. La station peut alors émettre des données de la classe

© Dunod – La photocopie non autorisée est un délit

asynchrone durant le temps THT et des données de la classe synchrone durant le temps Ts. Notons que, si toutes les stations utilisent leur temps d'émission de données de la classe synchrone, le temps de rotation du jeton est de 2 · TTRT.

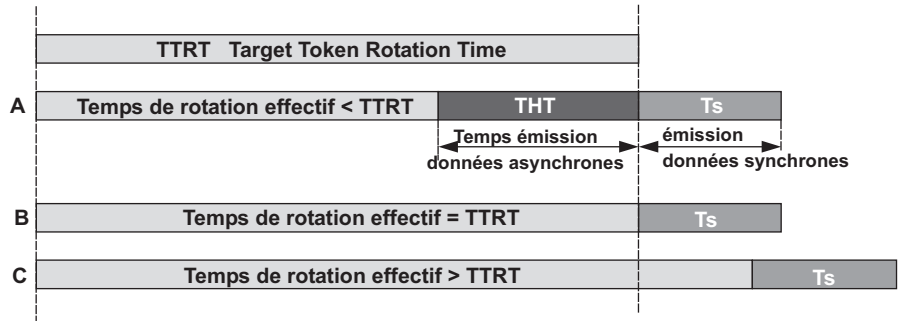


Figure 13.3 Gestion des temps d'émission.

La figure 13.3 représente ces variables dans différents cas, les valeurs sont celles vues d'une station. En **A**, le temps de rotation effectif du jeton est plus petit que TTRT, la station émet des données de la classe synchrone pendant Ts (les données synchrones sont toujours émises en premier) et de la classe asynchrone pendant THT (la figure matérialise des temps d'émission et non l'ordre d'émission). En **B** et **C** le temps de rotation effectif est égal ou plus grand que TTRT, la station ne peut émettre que des données synchrones.

Gestion des variables d'état

Les figures 13.4 et 13.5 représentent l'évolution des variables maintenues par une station. Dans l'hypothèse de la figure 13.4, à des fins de simplification, nous avons considéré que la station n'avait pas de données à émettre. Sur la figure 13.4, en t_0, la station initialise ses variables (TRT = TTRT, THT = 0, LC = 0). En t_1, la station reçoit un jeton, elle réinitialise ses variables : le jeton est en avance (TRT > 0) la variable THT (temps d'émission asynchrone autorisé) est initialisée à la valeur THT = TRT (temps restant) et la variable TRT est réinitialisée à TTRT (TRT mesure l'avance du jeton).

En t_3, le temporisateur TRT est échu et aucun jeton n'a été reçu : le jeton est en retard ; la variable LC est positionnée à 1 et la variable TRT est réinitialisée à TTRT. En t_4, le jeton arrive alors que TRT > 0, la variable LC étant positionnée, cette arrivée est une arrivée en retard. Par conséquent, l'émission de données asynchrones est impossible, le temporisateur TRT n'est pas réinitialisé et LC est réinitialisée à 0. Remarquons que si le jeton était arrivé après l'échéance de TRT, LC étant déjà à 1, une condition d'erreur aurait été détectée et l'anneau réinitialisé. En t_5, le jeton arrivant alors que TRT n'est pas achevé, le TRT est réinitialisé.

Sur la figure 13.5, à l'arrivée du jeton en t_1, la station possède des données synchrones et asynchrones à transmettre. Le compteur THT (temps d'émission des données asynchrones) est initialisé au temps restant (avance du jeton). La station émet ses données synchrones (le compteur THT n'est pas décrémenté) durant le temps imparti maximal Ts (rappelons que Ts représente une proportion du temps TTRT, il est le même pour toutes les stations), puis les données asynchrones durant le temps maximal autorisé (THT).

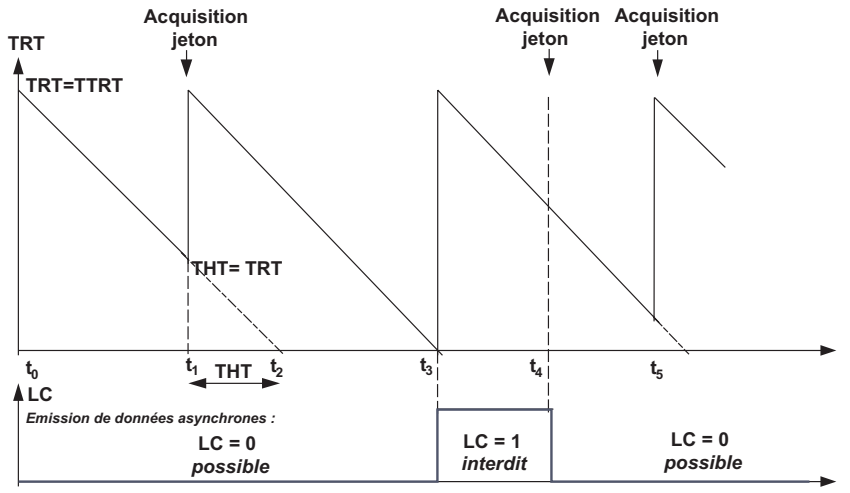


Figure 13.4 Gestion des variables d'état, sans émission de données.

À l'échéance de TRT (t_4), le jeton n'étant pas de retour, la variable LC est positionnée et TRT est réinitialisé. Le jeton arrive en t_5, seules des données synchrones peuvent être émises (LC = 1, à l'arrivée du jeton), TRT n'est pas réinitialisé (LC = 1) mais, LC est réinitialisé (LC = 0).

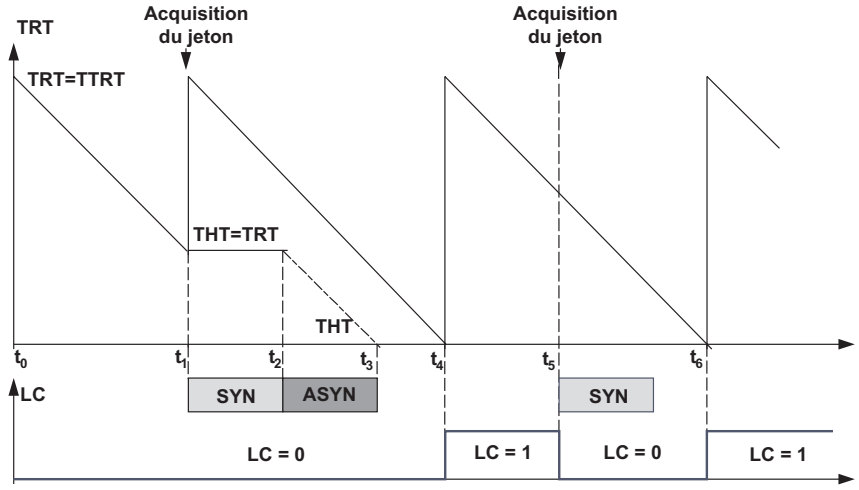


Figure 13.5 Gestion des variables d'état, avec émission de données.

13.1.3 Architecture du réseau FDDI

La figure 13.6 modélise l'architecture protocolaire du réseau FDDI. La couche physique est scindée en deux sous-couches, l'une (**PMD**, *Physical Medium Dependent*) réalise l'adaptation entre les organes d'émission (transducteurs optiques, connecteurs...) et le support physique utilisé (type de fibre optique, paires torsadées) ; l'autre gère le protocole physique (**PHY**, *PHYsical layer protocol*) et assure le codage des données et la synchronisation.

© Dunod – La photocopie non autorisée est un délit

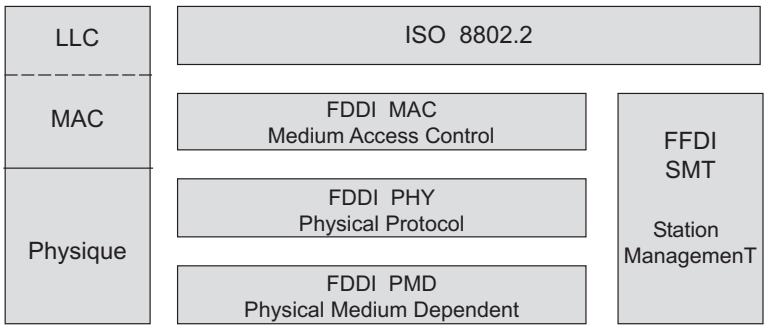


Figure 13.6 Architecture de FDDI.

La couche MAC est chargée des fonctions habituelles (gestion du jeton, temporisation...). Un protocole spécifique (**SMT**, *Station ManagemenT*) gère l'insertion et le retrait des stations, la configuration du réseau et le traitement des erreurs.

13.1.4 Aspects physiques

En fonction de leur mode de raccordement au support d'interconnexion, FDDI distingue deux types de stations : les stations à simple attachement (**SAS**, *Single Attachment Station*) et celles à double attachement (**DAS**, *Double Attachment Station*). Ces dernières sont reliées directement à l'anneau principal, tandis que les stations à simple attachement utilisent un concentrateur qui peut être à simple ou double raccordement (**SAC**, *Single Attachment Concentrator*, **DAC**, *Double Attachment Concentrator*).

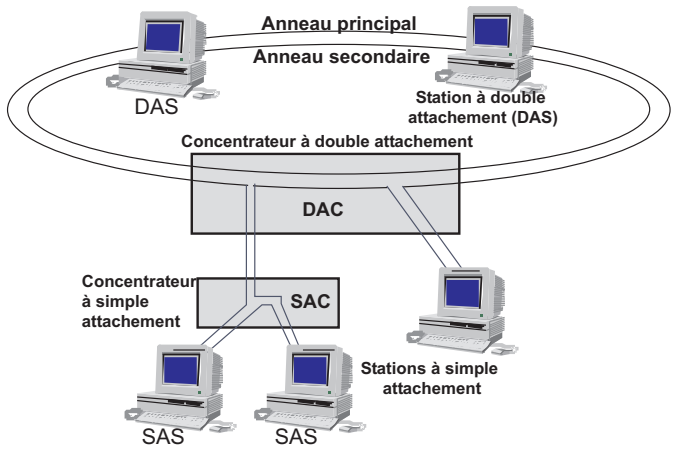


Figure 13.7 Topologie du réseau FDDI.

En cas de défaillance d'un nœud FDDI, le double anneau autorise le rebouclage sur l'anneau secondaire (cicatrisation). Pour les stations à simple attachement, cette fonction est assurée par le concentrateur (figure 13.7).

Le codage Manchester, utilisé dans Ethernet, génère deux états par temps bit. La rapidité de modulation est de 20 MBauds, d'où une horloge à 20 MHz (fréquence des données sur le support 10 MHz). Un même codage en FDDI conduirait à une fréquence d'horloge de 200 MHz

et une rapidité de modulation de 200 MBauds. Pour limiter la sollicitation des sources lumineuses, le codage utilisé est du type **NRZI** (*No Return to Zero Inverted*, non-retour à zéro inversé).

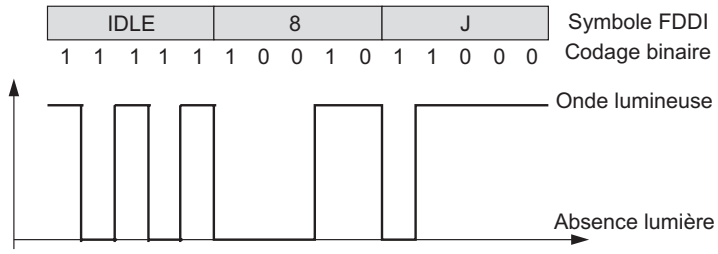


Figure 13.8 Codage NRZI.

Dans le codage NRZI représenté figure 13.8, il y a présence de transition à chaque un et pas de transition pour un zéro. De ce fait, les longues séquences de zéros n'offrent aucun repère de synchronisation (perte de la synchronisation bit). Pour y remédier, FDDI utilise un double codage : à une séquence de 4 bits, on fait correspondre une séquence de 5 bits, telle qu'il existe au moins deux transitions par symbole (code 4B/5B).

Combinaisons binaires 4B	Symboles FDDI 5B	Nom	Signification
	00100	H	Halt (permet d'arrêter l'activité sur l'anneau)
	11111	I	Idle (caractère de bourrage, synchronisation)
	11000	J	Délimiteur de trames
	10001	K	Délimiteur de trames
	00101	L	Délimiteur de trames (FDDI version 2)
	00000	Q	Quiet (absence de transition)
	00111	R	Zéro logique (Reset)
	11001	S	Un logique (Set)
	01101	T	Délimitation de trames
0000	11110	0	
0001	01001	1	
0010	10100	2	
0011	10101	3	
0100	01010	4	
0101	01011	5	
0110	01110	6	
0111	01111	7	
1000	10010	8	
1001	10011	9	
1010	10110	A	
1011	10111	B	
1100	11010	C	
1101	01010	B	
1110	01110	E	
1111	01111	F	

Figure 13.9 Codage et symboles de FDDI.

Ce double codage utilise 5 bits soit 32 symboles pour représenter 16 combinaisons binaires. Certains symboles disponibles sont utilisés pour la signalisation. Les combinaisons ne présentant pas au moins deux transitions sont invalides et inutilisées (sauf pour les symboles Quiet

© Dunod – La photocopie non autorisée est un délit

et Halt). Le tableau de la figure 13.9 fournit le codage 4B/5B utilisé par FDDI. Du fait de la transformation 4B/5B, les longueurs de champs de la trame FDDI s'expriment en nombre de symboles et non en nombre d'octets.

13.1.5 Format des trames FDDI

FDDI n'utilise qu'un seul type de trame (figure 13.10). Le champ **FC** (*Frame control*) distingue les trames de gestion (Trames MAC) des trames de données (trames LLC) et des trames d'administration (SMT).

PA	SD	FC	DA	SA	Données	FCS	ED	FS
16 sym.	2 sym.	2 sym.	4 ou 12 sym.	4 ou 12 sym.		8 sym.	2 sym.	$\geqslant$ 3 sym.

Figure 13.10 Format de la trame FDDI.

Les différents champs de la trame FDDI représentée figure 13.10 sont :

- le champ **PA**, préambule d'au moins 16 symboles *Idle*, l'indépendance des horloges émission de chaque station justifie la longueur relativement importante de la séquence de synchronisation bit ;
- le champ **SD** (*Start Delimiter*) ou synchronisation, ce caractère délimite le début de la trame FDDI (symboles I et J) ;
- le champ **FC** (*Frame Control*) indique le type de trame ; le tableau de la figure 13.11 fournit la signification de chacun des bits de ce champ ;
- les champs **DA** (*Destination Address*) et **SA** (*Source Address*) fournissent les adresses destination et origine. FDDI permet l'utilisation simultanée d'adressage IEEE long (6 octets ou 12 symboles) et court (2 octets ou 4 symboles), la longueur des champs adresses est précisée par le bit **L** du champ **FC** (L = 0 adresse sur 16 bits, L = 1 adressage long sur 48 bits). À l'instar du 802.5[1], le bit I/G du champ *Source Address* à 1, valide le champ *source routing* ;
- le champ données n'est présent que dans les trames LLC ;
- le champ **FCS** (*Frame Check Sequence*) protège les données et les champs FC, DA, SA ;
- le champ **ED** (*End Delimiter*), fanion de fin de trame (symboles T et E) ;
- enfin, comme en 802.5, le champ de statut de trame (**FS**) comporte les indications d'erreur, d'adresse reconnue et de trame recopiée. Il contient au moins trois symboles respectivement désignés E (erreur détectée), A (adresse reconnue) et C (trame recopiée). Chacun de ces symboles est mis au 0 logique par l'émetteur de la trame (symbole R) ; la station qui détecte une erreur positionne le champ E au 1 logique (symbole S). De même, chaque station qui reconnaît son adresse positionne le champ A à 1 logique (symbole S) et si elle recopie correctement la trame, le champ C à 1 logique (symbole S), ce bit sert d'acquittement mais aucune reprise n'est réalisée, si A = 1 et C = 0, une éventuelle reprise sera effectuée par les couches supérieures ; sinon ce champ reste à 0 logique (symbole R).

1. Routage par la source, voir section 12.4.2.

FDDI utilise deux types de jetons : le jeton normal, qui peut être utilisé par toutes les stations et le jeton réduit (ou jeton restreint). Ce dernier permet de réserver l'émission de données de la classe asynchrone à un groupe de stations. Le processus est initialisé par les couches supérieures afin d'offrir, à un moment donné, une bande passante plus large à ce groupe de stations.

	Frame Control				Signification
Bits	C	L	TT	ZZZZ	
	1	0	00	0000	Jeton libre
	1	1	00	0000	Jeton réduit
	C	L	00	0001 à 1111	Trame SMT (C = 0) Trame MAC (C = 1)
	C	L	01	rPPP	Trame LLC de priorité PPP

Figure 13.11 Détail du champ Frame Control.

Le champ FC (figure 13.11) permet de distinguer le type de transfert effectué (bit C, classe de transfert, à 0 il indique un transfert de la classe asynchrone et à 1 un transfert de la classe synchrone). Le bit L indique la longueur du champ adresse, (L = 0 adresse sur 16 bits, L = 1 adresse sur 48 bits). Les bits TT indiquent le type de trame, ils sont complétés par les bits ZZZZ qui, dans une trame de données, peuvent éventuellement indiquer un niveau de priorité. FDDI autorise 8 niveaux de priorité (3 bits), le bit r est réservé à un usage ultérieur.

13.1.6 Fonctionnement général de l'anneau

À l'initialisation, une station, sur détection d'inactivité, émet une requête d'initialisation (*Claim Token*). La trame *Claim Token* indique la valeur du TTRT revendiqué. Chaque station recevant cette trame compare la valeur du TTRT avec celle qu'elle désire. Si cette valeur est inférieure à la valeur proposée, la station mémorise la valeur actuelle qu'elle remplace par la sienne. La station qui voit revenir sa proposition est considérée comme gagnante, ce qui correspond au TTRT le plus contraignant, en cas d'égalité entre deux stations c'est la station de plus forte adresse qui « gagne ». La station gagnante génère, alors un jeton pour informer toutes les stations du TTRT retenu. L'émission de données ne pourra avoir lieu que lors de l'émission du second jeton.

Une station qui a des données à émettre attend la réception d'un jeton. À réception de celui-ci, elle le répète jusqu'au délimiteur de début, insère ses données et régénère un nouveau jeton. À l'instar du réseau Token Ring, c'est la station qui a émis la trame qui la retire de l'anneau.

13.1.7 Évolution de FDDI : FDDI-II

FDDI offre une bande passante minimale aux données de la classe synchrone mais ne garantit pas une récurrence temporelle entre les différentes émissions. De ce fait, FDDI n'est pas susceptible d'assurer des transferts de données de type isochrone (voix, vidéo). Pour pallier cette limitation une évolution de FDDI a été proposée.

Il s'agit de FDDI-II qui multiplexe sur le support, une voie asynchrone et synchrone (fonctionnement en mode paquets) et une voie isochrone (fonctionnement en mode circuits). La figure 13.12 présente l'architecture générale du réseau FDDI-II.

© Dunod – La photocopie non autorisée est un délit

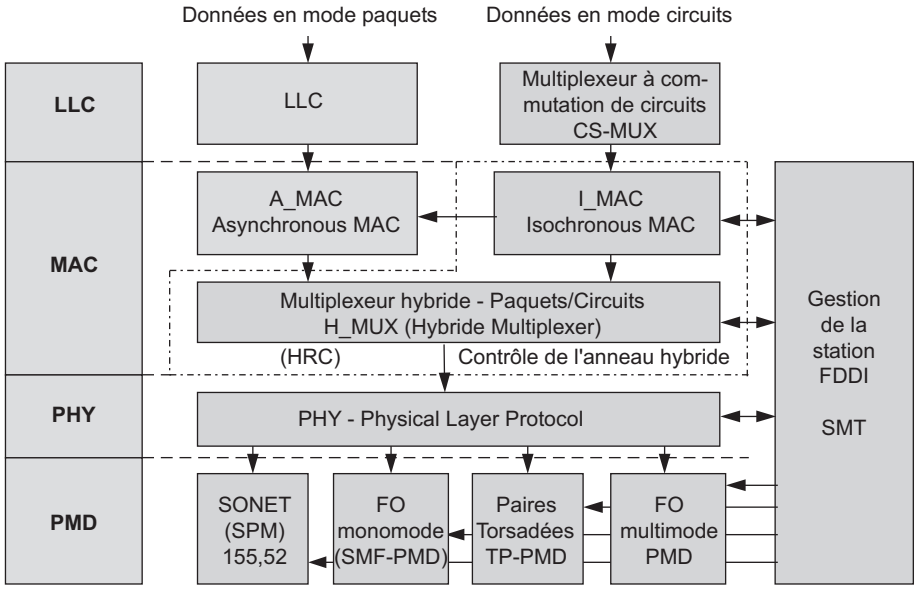


Figure 13.12 Architecture du réseau FDDI-II.

Si le trafic généré n'est que du type paquet, une station FDDI-II fonctionne en mode de base, lorsque du trafic paquet et du trafic isochrone sont multiplexés sur le support elle fonctionne en mode hybride. Une station maître (Cycle Master) génère une trame ou cycle FDDI-II toutes les 125 μs soit 12 500 bits.

13.1.8 Conclusion

FDDI a toujours eu du mal à se positionner entre les LAN et le MAN. La version 2 arrivée trop tard n'a connu aucun succès.

13.2 DQDB (DISTRIBUTED QUEUE DUAL BUS)

13.2.1 Généralités

Issu des laboratoires de l'université de Western Australia et soutenu par les télécommunications australiennes (Telecom Australia), le réseau QPSX (*Queue Packet Dual Bus*) a été normalisé par l'IEEE et l'ISO (IEEE 802.6, IS 8802.6) comme réseau métropolitain (MAN) sous le nom de **DQDB** . Cependant, la norme ne précise aucune limite en distance.

Développé parallèlement à **ATM** (*Asynchronous Transfer Mode*), DQDB en utilise le format (cellule de 53 octets dont 48 de charge utile). DQDB est parfois considéré comme une technologie pré-ATM. Il permet le transfert de données isochrones et asynchrones (mode connecté et non connecté). Les débits actuellement offerts sont de 45, 155 et 622 Mbit/s.

DQDB utilise un double bus unidirectionnel (figure 13.13). Sur chaque bus, une tête de bus (**HoB**, *Head of Bus*) génère, toutes les 125 μs, une trame (trame DQDB) contenant n slots ou

cellules de 53 octets. Le nombre de slots par trame (n) dépend du débit du réseau. Le premier bit de chaque slot (bit Busy) indique l'état du slot (libre ou occupé).

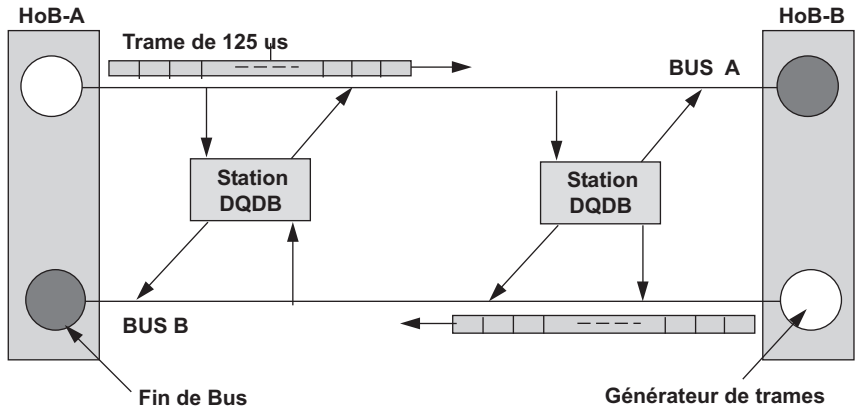


Figure 13.13 Principe général du réseau DQDB.

Chaque station, qui a des données à émettre, les dépose dans un slot vide attribué de manière statistique pour le transfert de données asynchrones ou selon un préarbitrage, pour les données isochrones. La topologie est un anneau physique, les têtes de bus (HoB) étant situées sur une même station (figure 13.14).

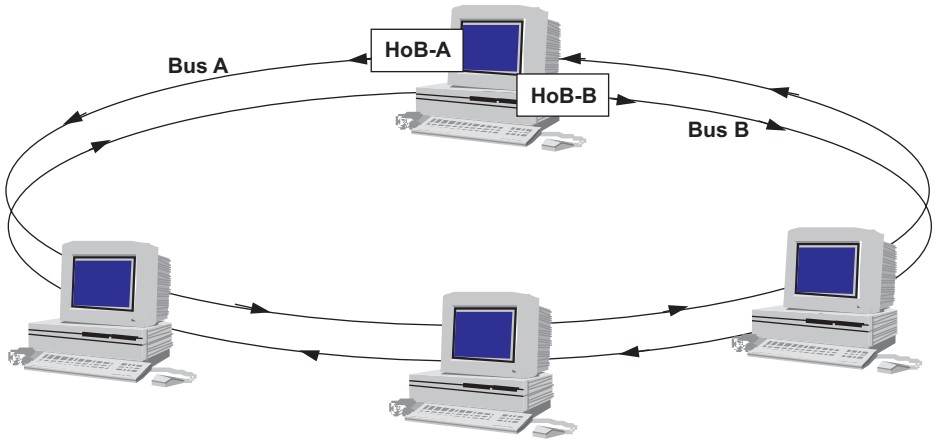


Figure 13.14 Topologie physique de DQDB.

Une station lit ou écrit au vol les données (fonction « OU logique ») dans une cellule ; elle ne les retire pas, la cellule les contenant s'évanouit en fin de bus (fonction d'absorption). Les stations sont à l'écoute des deux bus (bus A et bus B). Du fait de ce double raccordement, l'architecture DQDB définit deux points d'accès au service physique, un par bus (figure 13.15). L'émission n'a lieu que sur un seul bus en fonction de la position physique de la station avec laquelle elles veulent communiquer. Les messages de diffusion (broadcast) sont émis sur les deux bus.

© Dunod – La photocopie non autorisée est un délit

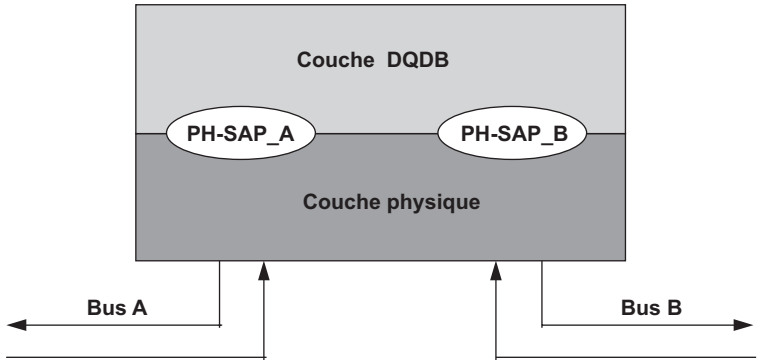


Figure 13.15 Point d'accès au service physique de DQDB.

13.2.2 Architecture générale de DQDB

DQDB offrant trois types de service : transfert asynchrone en mode connecté et non connecté et le transfert isochrone. La couche MAC comprend un ensemble de fonctions spécifiques à chaque type de transfert (figure 13.16) :

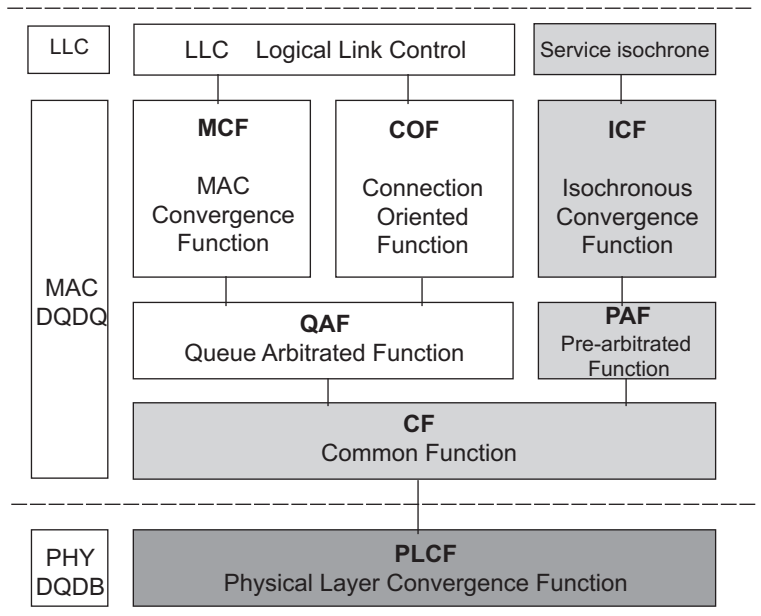


Figure 13.16 Architecture du réseau DQDB.

– **MCF** (*MAC Convergence Function*) offre un service asynchrone sans connexion (service de type datagramme) qui est particulièrement adapté aux transferts en mode rafales (transfert de données entre ordinateurs) ;

– **COF** (*Connection Oriented Function*) : ce service, comme le précédent, est dédié aux transferts asynchrones mais en mode connecté. Un circuit virtuel (mode orienté connexion) est

établi préalablement à l'échange de données. Ce type de service est essentiellement destiné aux applications de type conversationnel ;

– **ICF** (*Isochronous Convergence Function*) offre un service de transfert de type isochrone qui garantit un débit constant et une récurrence parfaite entre les blocs de données transportés. Ce service est destiné aux applications de type voix et vidéo.

L'accès au support partagé est géré par deux entités : l'une prend en charge le trafic isochrone (**PAF**, *Pre-Arbitrated Function*) et l'autre le trafic asynchrone (**QAF**, *Queue Arbitrated Function*).

13.2.3 Algorithme d'accès au support

Transfert isochrone (accès préarbitré)

Pour le trafic isochrone, l'allocation des cellules est gérée par la tête de bus. Un protocole de signalisation spécifique (Q.931 du RNIS bande étroite) établit un lien virtuel (**VC**, *Virtual Connection*) entre les stations participant à l'échange isochrone (point à point ou point à multipoint).

Lors de la demande d'établissement, selon le débit requis par la station source la tête de bus alloue une ou plusieurs cellules (cellules **PA**, *Pre-Arbitrated*). L'affectation d'une cellule, dans une trame, peut garantir un débit de 3 072 kbit/s (8 000 cellules de 48 octets par seconde). Pour éviter une perte de bande passante, DQBD peut multiplexer plusieurs connexions dans une même cellule (1 octet de la cellule garantit un débit de 64 000 bit/s). Lors de la demande d'établissement d'une connexion, la tête de bus attribue un identifiant de circuit (**VCI**, *Virtual Circuit Identifier*) et détermine la position des données dans la cellule. Ces deux informations, VCI et position, identifient complètement une connexion.

Transfert asynchrone (accès statistique)

À la différence du trafic isochrone, le trafic asynchrone est géré par chaque station. En mode connecté, c'est la station effectuant la demande de connexion qui détermine l'identifiant de circuit (VCI). En mode non connecté, tous les bits du champ VCI sont positionnés à 1. Le principe d'accès au support repose sur une gestion distribuée des files d'attente (DQDB) qui garantit au trafic asynchrone un délai d'accès déterministe. Le principe exposé ci-dessus permet de réserver, à chaque station, un débit minimal.

Supposons une station désirant émettre sur le bus A, elle formule une requête de réservation sur le bus B. Le choix du bus est défini en fonction de la position relative de la station destination par rapport à la station source.

➤ Détermination de la position relative de la station

La figure 13.17 illustre le mécanisme de détermination de la position relative de la station. Pour déterminer où est située la station destination, la station *Y* émet un message à destination de *X* (message D) sur les deux bus. La station *X* en fonction du bus de réception, répond à la station *Y* (message R), la station *Y* apprend ainsi la position de la station *X*.

© Dunod – La photocopie non autorisée est un délit

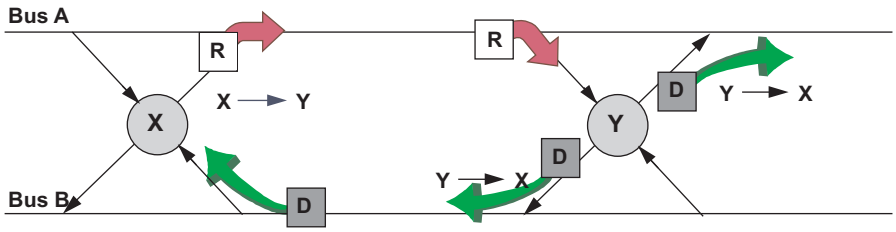


Figure 13.17 Détermination de la position des stations.

➤ Principe de l'accès

Chaque station décompte en permanence les requêtes émises par les stations amont. Si une station a dénombré *N* requêtes de réservation sur le bus B, elle laissera passer *N* slots vides sur le bus A avant de déposer ses données dans le slot vide *N* + 1. La figure 13.18 illustre ce principe.

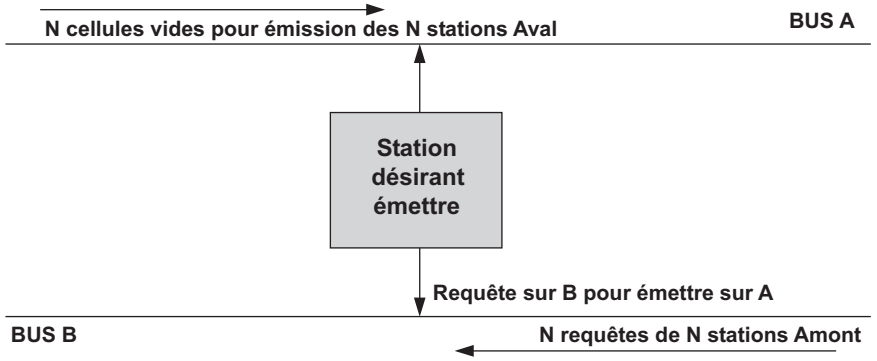

N cellules vides pour émission des N stations Aval
BUS A
Station désirant émettre
Requête sur B pour émettre sur A
BUS B
N requêtes de N stations Amont

Figure 13.18 Principe de gestion de l'accès distribué au support.

Ce procédé ne partage pas équitablement la bande passante. En effet, les stations en amont émettent leurs requêtes de réservation avant, elles sont donc favorisées. Le mécanisme dit « *Bandwidth Balancing Mechanism* » tend à corriger ce défaut : lorsqu'une station a émis *n* segments, elle laisse passer obligatoirement une cellule vide. Ce mécanisme, d'origine ATT, a été adopté par l'IEEE.

➤ Étude détaillée du mécanisme d'accès

Chaque station maintient deux compteurs (figure 13.19) :

– un compteur de requêtes (**RQ**, *Request Counter*) incrémenté de 1 à chaque nouvelle requête identifiée et décrémenté de 1 à chaque cellule vide identifiée sur le bus d'émission (satisfaction d'une requête), le compteur RQ comptabilise ainsi les requêtes non satisfaites ;

– un compteur décrémental (**CD**, *Count Down Counter*), décrémenté de 1 à chaque cellule vide est identifiée sur le bus d'émission.

Lorsqu'une station désire émettre, elle :

– transfère le contenu du compteur de requêtes (demandes en amont d'émission non satisfaites) dans le compteur décrémental (CD) ;

– réinitialise à zéro le compteur de requêtes (RQ) ;
– émet une requête sur le bus sélectionné (CD) ;
– décrémente le compteur décrémental à chaque cellule vide identifiée sur le bus d'émission ;
– place ses données dans la première cellule disponible sur le bus sélectionné pour l'émission, dès que le compteur décrémental est à zéro (CD).

Une requête ne peut être formulée que si la précédente a été satisfaite et qu'elle ne concerne qu'un seul segment de données. La figure 13.19 illustre la gestion des compteurs, la station désire émettre sur A, elle formule sa requête sur B.

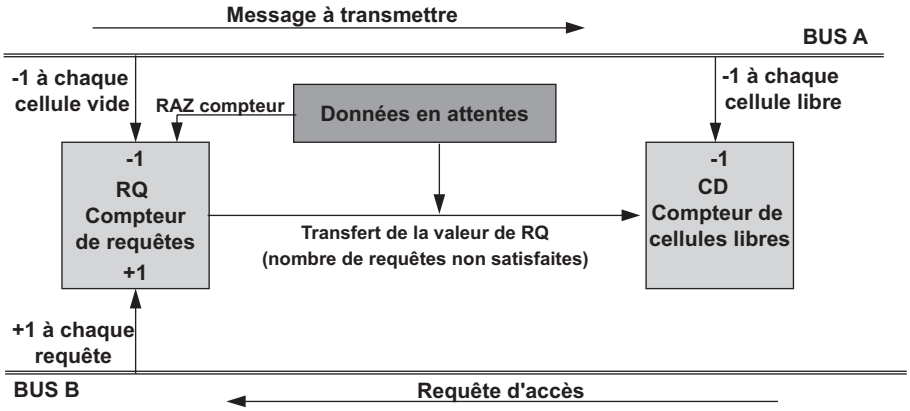


Figure 13.19 Principe de gestion des compteurs d'une station.

13.2.4 Format de l'unité de donnée DQDB

La structure de données DQDB est relativement complexe, elle est représentée figure 13.20. La trame MAC de 0 à 9 188 octets (**SDU**, *Service Data Unit*) est encapsulée dans une unité de protocole **IM-PDU** (*Initial MAC Protocol Data Unit*). Celle-ci est ensuite segmentée en fragments de 48 octets dont 44 de charge utile (**DM-PDU**, *Derived MAC PDU*). La DM-PDU est ensuite encapsulée pour former un segment DQDB (52 octets), un octet de contrôle d'accès est ajouté pour obtenir le slot DQDB (53 octets).

Le slot DQDB a une charge utile maximale de 48 octets. Son format est commun au trafic asynchrone (slot QA) et isochrone (slot PA). L'en-tête de 5 octets comprend l'octet de contrôle d'accès (**ACF**, *Access Control Field*) et 4 octets de gestion de la charge utile. **L'ACF**, *Access Control Field*, comporte :

– le bit **BB**, *Busy Bit*, qui indique l'état de la cellule (libre BB= 0, occupée BB= 1) ;
– le bit suivant (**ST**, *Slot Type*) précise le type de slot (ST = 0 pour un slot QA et ST = 1 pour un slot PA) ; ce bit n'a de sens que lorsque le bit BB est positionné à 1 ;
– le bit **PSR** (*Previous Slot Received*) est positionné par la station suivant le destinataire lorsque ce dernier a lu le message (lecture du slot précédent), il devrait permettre la réutilisation d'un slot lu. Ce bit est non utilisé ;

© Dunod – La photocopie non autorisée est un délit

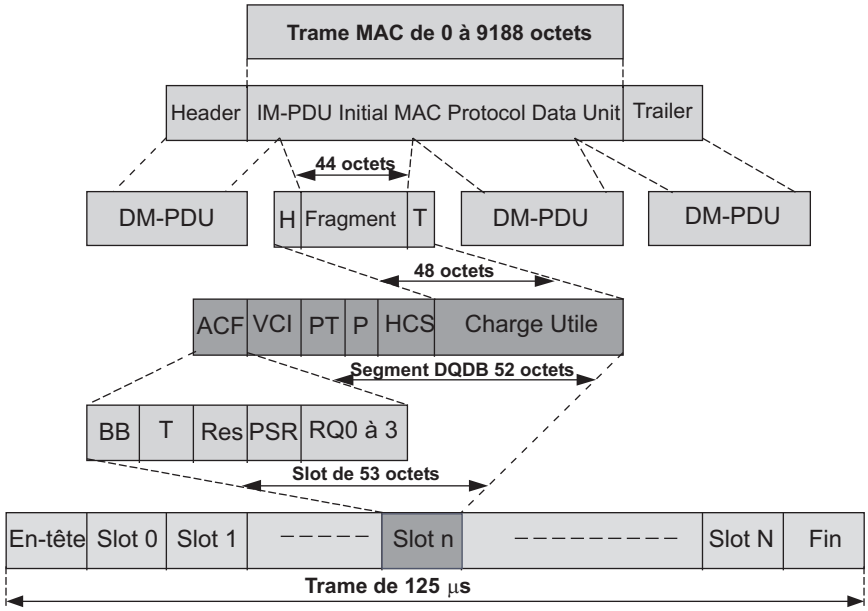


Figure 13.20 Format du slot DQDB.

– le bit suivant est inutilisé, il est réservé à une utilisation ultérieure (*Res*) ;
– les quatre derniers bits (**RQ**, *Request bit*) permettent de formuler des requêtes de réservation suivant un certain niveau de priorité (bit RQ0 priorité basse à RQ3 priorité haute).

Les 4 octets de gestion suivants comportent :

– les informations d'identification du **VCI** (*Virtual Circuit Identifier*) sur 20 bits. Le VCI est attribué par une station spécifique (serveur de VCI). L'ouverture et la fermeture de circuits isochrones sont contrôlées par le protocole de signalisation Q.931. En mode non connecté, tous les bits du champ VCI sont à 1. En attribuant différentes valeurs disponibles de VCI à un ensemble de stations on peut réaliser des réseaux virtuels garantissant une certaine sécurité aux données ;
– les informations relatives au type de charge, champ **PT** (*Payload Type*), sur 2 bits ; ce champ indique le type de données transportées (00 pour les données utilisateurs) ;
– puis, 2 bits indiquent la priorité du segment. Lors du raccordement du réseau vers un réseau extérieur, le champ **P** (*Segment Priority*) permet la mise en œuvre d'un mécanisme de contrôle de congestion ;
– enfin, le champ **HCS** (*Header Check Sequence*) réalise un contrôle d'erreur limité à l'en-tête selon la technique du polynôme générateur (CRC8).

13.2.5 Le service SMDS et CBDS

D'origine Bellcore, la proposition **SMDS** (*Switched Multimegabits Data Service*) reprise en Europe sous l'appellation **CBDS** (*Connectionless Broadand Data Service*) qui offre un service d'interconnexion de réseaux en mode non connecté. S'appuyant sur l'AAL5 d'ATM, SDMS

offre une interface utilisateur similaire à celle de DQDB. SMDS a souvent été perçu comme une solution d'accès provisoire aux réseaux ATM. Cette solution a surtout été mise en œuvre pour l'interconnexion des réseaux locaux.

13.3 LES RÉSEAUX LOCAUX ATM[2]

13.3.1 Généralités

Apporter, jusqu'au poste de travail des utilisateurs d'un réseau local, la bande passante ATM n'est envisageable que si son environnement de travail ne s'en trouve pas modifié, or les normes ATM et LAN diffèrent.

Les applications, systèmes d'exploitation et protocoles utilisés dans les réseaux locaux ne peuvent fonctionner en natif sur les réseaux ATM. De plus, ATM offre un service orienté connexion, les réseaux locaux utilisent le mode non connecté et la diffusion générale (broadcast) ou partielle (multicast). Enfin, les réseaux locaux utilisent un adressage à plat ou global (IEEE), ATM un adressage hiérarchique de type E.164 (UIT-T) ou NSAP (ISO).

Le nombre de réseaux locaux et d'applications exploitant les technologies LAN et la pile de protocoles TCP/IP fait que l'introduction d'ATM dans ces environnements n'est envisageable que si cela n'induit que peu de modifications de l'existant. Or, pour tirer pleinement parti de toutes les potentialités d'ATM (garantie de qualité de service de bout en bout), il faudrait introduire cette technologie jusqu'au poste de travail de l'utilisateur final. Appuyer les applications directement sur ATM aurait un impact technique et financier considérable sur l'accès aux ressources réseau et sur les applications elles-mêmes. Pour ces raisons, il est primordial de masquer aux applications existantes la technologie ATM.

Deux problèmes sont alors à résoudre, la diffusion des messages propres au mode non connecté des réseaux locaux, et la réutilisation des piles protocolaires.

Aspect mode non connecté

L'émulation d'un service sans connexion peut être obtenue en spécialisant un ou plusieurs nœuds du réseau dans la diffusion des messages. Toutes les stations du réseau sont connectées via un circuit virtuel permanent à l'un de ces nœuds : le serveur sans connexion (**CLS**, *ConnectionLess Server*). Les différents serveurs sans connexion du réseau sont reliés entre eux par un faisceau de circuits virtuels permanents. Lorsqu'une station envoie des données, celles-ci sont adressées au serveur sans connexion, celui-ci prend en charge, pour le compte de la station source, le routage et la diffusion du message au destinataire.

Dans une telle architecture (figure 13.21), l'établissement d'un lien entre la source et le destinataire est devenu inutile (émulation du mode non connecté), mais le serveur sans connexion devient vite un goulet d'étranglement.

2. Avant d'étudier cette partie, il est recommandé de relire le chapitre concernant l'étude d'ATM (voir section 11.2.5).

© Dunod – La photocopie non autorisée est un délit

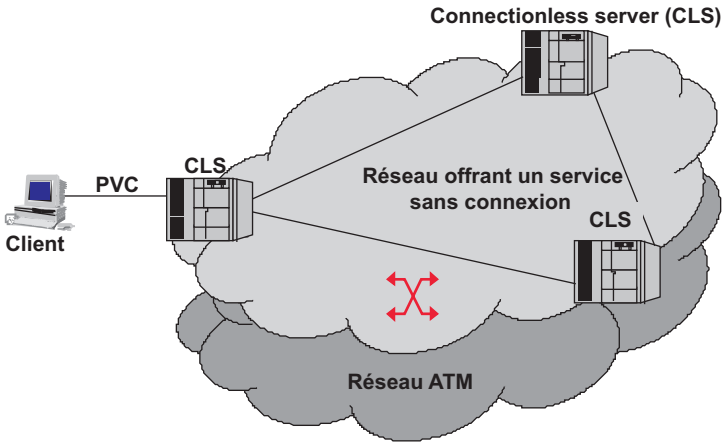


Figure 13.21 Principe du mode non connecté sur ATM.

Aspect protocolaire

Les réseaux locaux utilisent essentiellement le protocole IP du DoD. Traditionnellement, la communication entre stations d'un réseau local s'effectue après mise en correspondance de l'adresse réseau IP et de l'adresse MAC par le protocole **ARP** (*Address Resolution Protocol*). Dans les réseaux LAN ATM, ce sont les adresses IP et ATM qui doivent être mises en correspondance. Pour résoudre le problème d'adressage IP/ATM, deux solutions ont été envisagées (figure 13.22) :

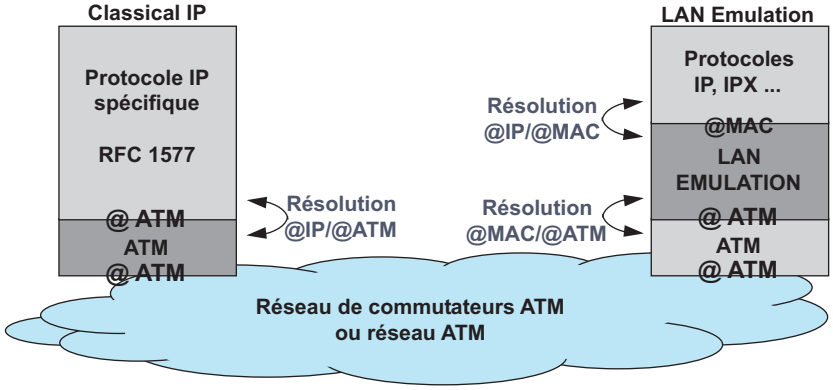


Figure 13.22 Les piles protocolaires sur les LAN ATM.

– l'IETF (*Internet Engineering Task Force*) propose la mise en œuvre d'une pile TCP/IP particulière qui effectue directement la mise en relation d'adresses IP avec des adresses ATM (RFC 1577, *Classical IP and ARP over ATM*). ATM est alors utilisé comme un système de transmission rapide puisque l'usage du protocole IP (V4) n'autorise pas l'exploitation des avantages procurés par ATM ;

– l'ATM Forum quant à lui préconise l'insertion, entre les services ATM et une pile IP traditionnelle, d'une couche interface chargée d'émuler les services d'un réseau local (*LAN*

Emulation). Cette couche présente, à la couche IP, une adresse MAC qu'elle met en relation avec l'adresse ATM de la station (double résolution d'adresses).

La compatibilité complète de l'implémentation d'IP sur ATM est l'avantage majeur de ces deux approches. Toutefois :

– seules les communications entre machines d'un même réseau logique peuvent communiquer directement et bénéficier de la garantie de service d'ATM ;
– le temps d'établissement des circuits virtuels pénalise les performances lors de transfert de données de faible taille ;
– tous les paquets entre deux systèmes partagent le même circuit virtuel, ce qui rend impossible de garantir à un flux spécifique une qualité de service spécifique.

13.3.2 « Classical IP » ou « IP over ATM »

Principes généraux

Classical IP (**CLIP**) ou mode natif définit un réseau IP comme un sous-réseau logique (**LIS**, *Logical IP Subnetworking*) de manière similaire à un réseau IP traditionnel. Un LIS (*Logical IP Subnetwork*) est un ensemble de machines IP connectées à un réseau ATM (figure 13.23) partageant un même préfixe d'adresse IP.

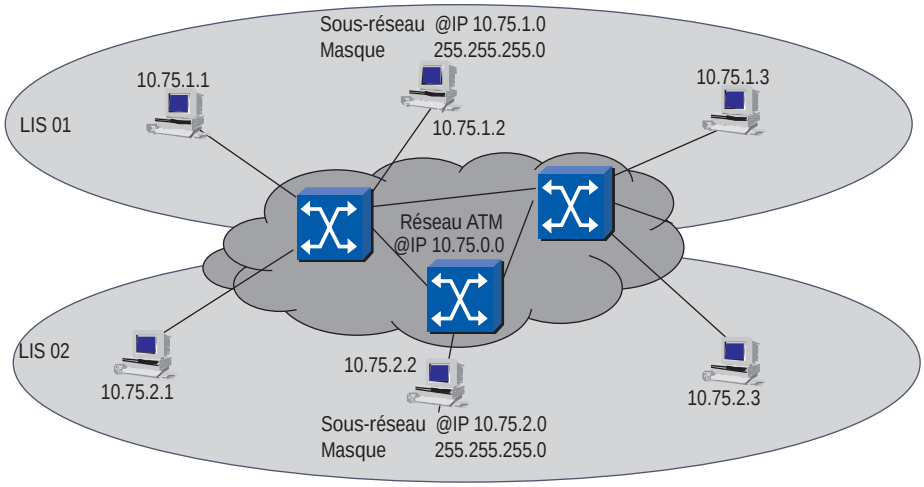


Figure 13.23 Principe du Classical IP.

Les stations d'un même sous-réseau (LIS) communiquent directement entre elles après avoir établi un circuit virtuel. Les stations de deux sous-réseaux différents communiquent via un routeur.

Communication intra-LIS

Pour la mise en relation directe des stations d'un même sous-réseau, chaque station client doit connaître les adresses IP et ATM du destinataire. La fonction de résolution d'adresses (mise en correspondance de l'adresse IP avec l'adresse ATM de la station) est assurée par un serveur

© Dunod – La photocopie non autorisée est un délit

d'adresses (serveur ATMARP) qui, sur sollicitation d'une requête **ATMARP** (*ATM Address Resolution Protocol*), renvoie au client l'adresse ATM correspondante. Chaque réseau logique (LIS) possède son propre serveur ATMARP (figure 13.24).

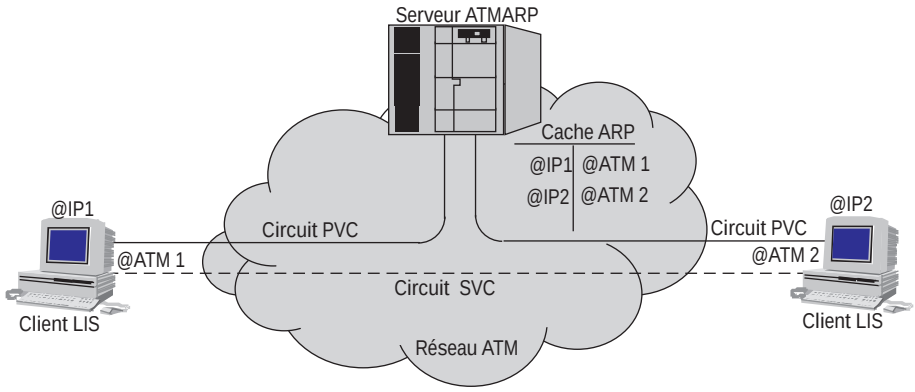


Figure 13.24 Principe d'un serveur ATMARP.

À la configuration d'un client LIS, celui-ci, outre son adresse ATM, est informé de l'adresse ATM du serveur ATMARP. Lors de sa connexion au réseau (figure 13.25), le client LIS établit un circuit virtuel permanent (**PVC**, *Permanent Virtual Circuit*) avec le serveur ATMARP. Ce dernier émet une requête InARP (Inverse ARP) pour connaître l'adresse IP de la station. Le serveur ATMARP met alors son cache ARP à jour (table de correspondance @IP/@ATM).

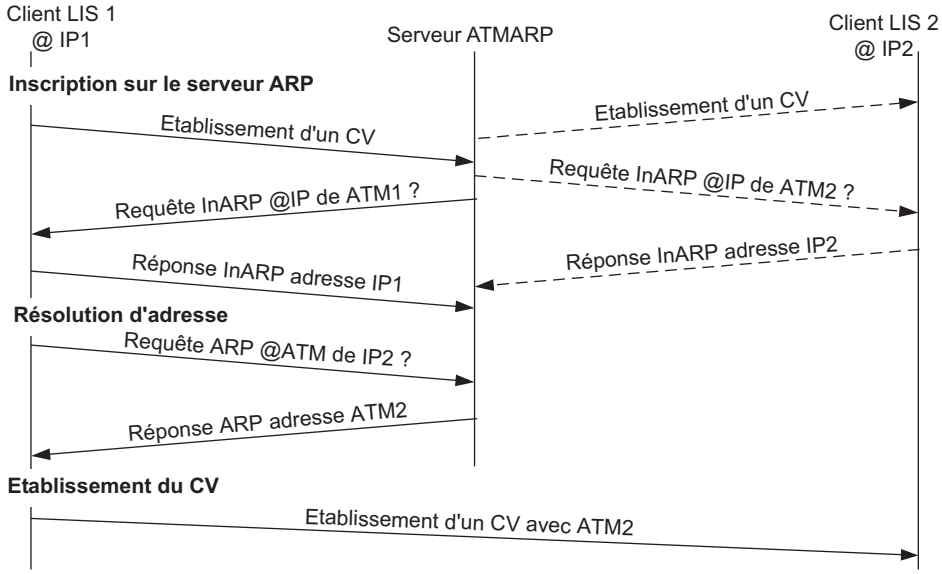


Figure 13.25 Établissement d'un circuit virtuel entre deux clients LIS.

Lorsqu'un client LIS veut entrer en relation avec un autre client du même LIS, il émet une requête ARP vers le serveur ATMARP (quelle est l'adresse ATM de la station IP ?), celui-ci lui fournit alors l'adresse ATM, le client LIS met son cache ATM à jour (@IP/@ATM), et établit un circuit virtuel commuté (**SVC**, *Switched Virtual Circuit*) avec cette station.

Communication inter-LIS

La communication entre stations de LIS différents transite par un ou plusieurs routeurs intermédiaires (figure 13.26). La mise en relation s'effectue en deux temps : la station source établit un circuit virtuel (SVC) avec le routeur, ce dernier à son tour établit un circuit avec la station destinataire ou un autre routeur. Le routeur entretenant un grand nombre de SVC constitue un goulet d'étranglement. Le fait de transiter, éventuellement, par plusieurs routeurs pénalise considérablement les performances.

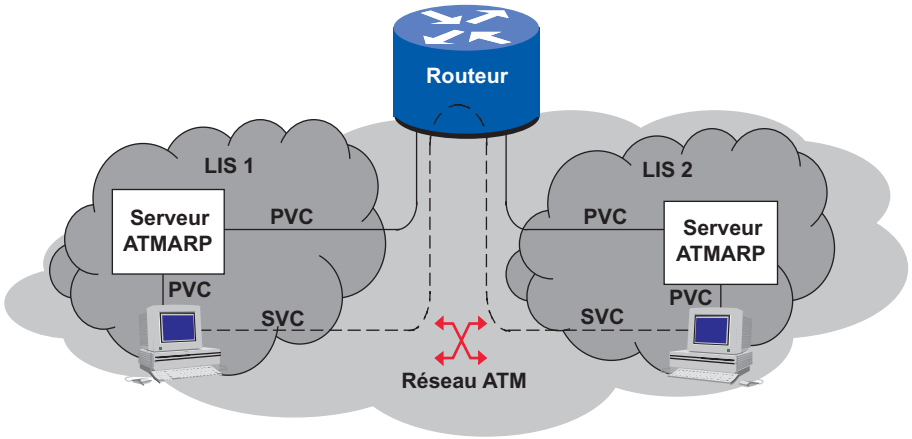


Figure 13.26 Principe de la communication inter-LIS.

Format des données (RFC 1 483)

Classical IP utilise AAL5 et la RFC 1 483 pour l'encapsulation des données. Dans la figure 13.27 le paquet IP subit une double encapsulation : LLC (*Logical Link Control*) et SNAP (*Subnetwork Access Protocol*) déjà décrite précédemment. C'est cette trame qui est remise à l'AAL5, le MTU est fixé à 9 180 octets.

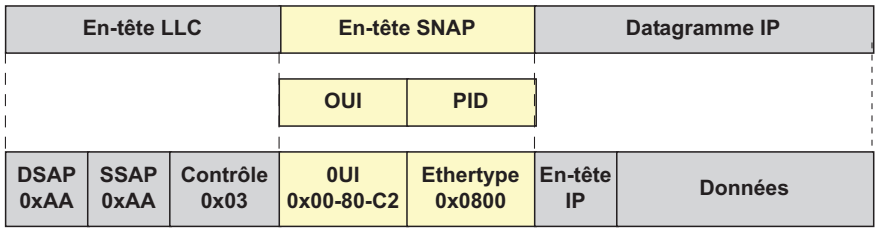


Figure 13.27 Format d'encapsulation RFC 1 483.

13.3.3 LAN Emulation

Généralités

Classical IP ne peut ni prendre en compte un trafic de multicast ou de broadcast ni communiquer avec les LAN traditionnels (*Legacy LAN*). La communication entre un *legacy* LAN et un LAN ATM nécessite, d'une part l'utilisation de protocoles communs et, d'autre part

© Dunod – La photocopie non autorisée est un délit

que les applications sur les LAN ATM voient le LAN ATM comme un réseau local traditionnel (Ethernet, Token Ring...). Cette approche conduit à introduire entre les services ATM et les protocoles réseaux une couche spécifique émulant, vis-à-vis des protocoles supérieurs, les fonctions d'un LAN traditionnel (figure 13.28).

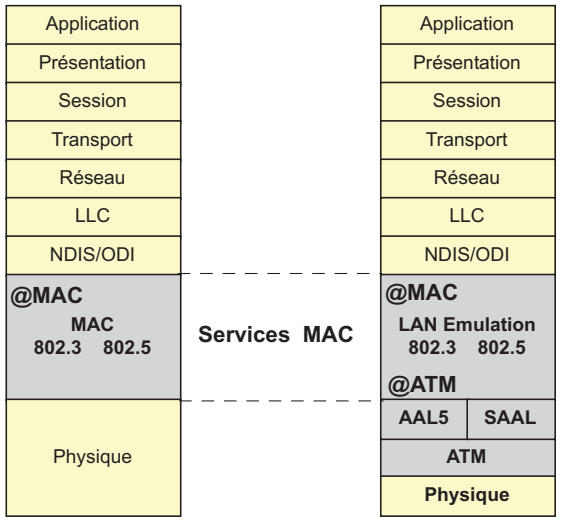


Figure 13.28 Architecture d'un LAN traditionnel et d'un LAN ATM.

L'interface LAN Emulation (**LUNI**, *LAN emulation User to Network Interface*) d'une station cliente (**LEC**, *LAN Emulation Client*) fournit un service MAC en mode non connecté aux couches supérieures. Cette interface a deux adresses, une adresse MAC vue des couches supérieures et une adresse ATM vue du réseau ATM. Le LEC utilise l'ALL5 pour le transfert des données et la SAAL (*Signaling* AAL) pour la signalisation (signalisation Q.2931), et en particulier pour l'établissement et la libération des circuits virtuels commutés (SVC).

Chaque LEC entretien un cache ARP (correspondance entre les adresses ATM et MAC des stations connues). Le LEC peut être configuré pour délivrer des trames MAC au format 802.3 ou 802.5, le champ FCS de la trame MAC n'est pas utilisé. Tous les LEC d'un même réseau émulé[3] (**ELAN**, *Emulated LAN*) doivent utiliser le même format de trames MAC. Un LEC ne peut appartenir qu'à un seul ELAN. Si un système d'extrémité doit être connecté à plusieurs ELAN, il possédera un LEC par ELAN rejoint et une interface physique ou logique par LEC.

Les composants d'un LAN ATM (ELAN)

Les différents nœuds d'un réseau local émulé (ELAN, *Emulated LAN*) constituent un réseau virtuel. Un réseau ATM peut supporter plusieurs ELAN (figure 13.29). Chaque ELAN est identifié par un nom (ELAN-ID). La fonction LEC (*LAN Emulation Client*) est présente dans tous les nœuds d'un ELAN. Les différents services d'un ELAN sont offerts par :

3. Ne pas confondre les termes ELAN et LANE. LANE *(LAN Emulation*) est la technique mise en œuvre sur ATM pour émuler, sur ce dernier, un réseau local (ELAN, *Emulated LAN*).

– le **LES** (*LAN Emulation Server*), similaire au serveur ATMARP du Classical IP, assure la mise en relation d'une adresse MAC et d'une adresse ATM. Cette fonction est généralement localisée dans un commutateur ATM. Il y a un LES par ELAN ;
– le **BUS** (*Broadcast and Unknown Server*) fournit les services de diffusion aux trames MAC de diffusion (broadcast ou multicast). Il est aussi chargé de la résolution d'adresses pour les LEC non connus du LES (diffusion d'une requête LE-ARP). Les fonctions du BUS sont réalisées par le même commutateur que les fonctions LES. Il y a un serveur BUS par ELAN. Chaque LEC entretient une connexion permanente avec le serveur BUS. Si le LAN émule un réseau Token Ring, le BUS émule l'anneau en assurant le passage des trames (jeton compris) de système terminal à système terminal selon un ordre préétabli ;
– enfin, le **LECS** (*LAN Emulation Configuration Server*) fournit un service d'autoconfiguration de type « *plug and play* ». Sur la requête d'un LEC, le LECS affecte le LEC à un ELAN en lui fournissant l'adresse du LES pour qu'il puisse s'enregistrer auprès de ce dernier. Un LEC ne peut appartenir qu'à un seul ELAN. Le LECS est commun à tous les ELAN du réseau ATM.

Les échanges inter-ELAN doivent transiter par un pont ou un routeur. La figure 13.29 décrit la topologie générale d'un LAN ATM.

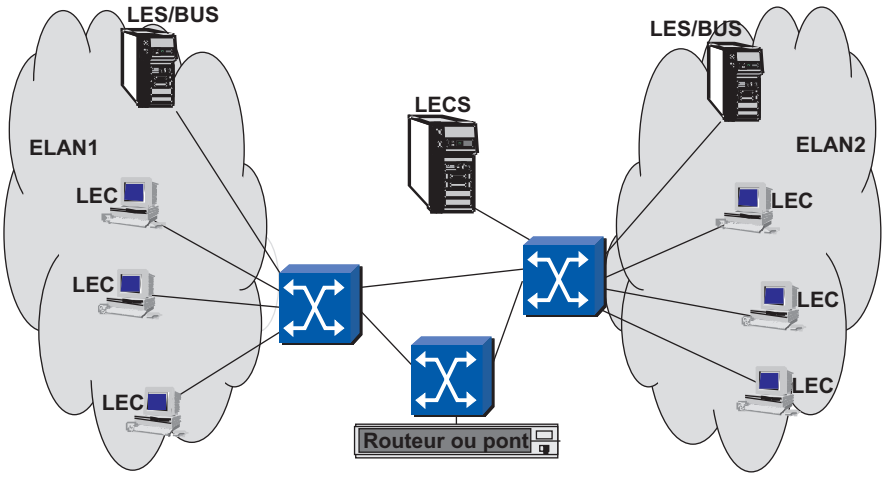


Figure 13.29 Topologie d'un LAN ATM.

Fonctionnement des ELAN (Emulated LAN)

Pour transférer des données entre deux clients, il faut établir une connexion (*Data Direct VCC*). Pour cela le LEC source doit disposer de certaines informations qui lui ont été fournies, à la configuration du système, par l'administrateur. Il s'agit notamment de sa propre adresse ATM et de l'identifiant de son ELAN de rattachement (ELAN-ID). D'autres informations lui sont fournies par le **LES** (*LAN Emulation S*erver) de son ELAN auprès duquel il doit s'enregistrer (résolution d'adresses) et obtenir l'adresse ATM du destinataire. Cette procédure très complexe est décrite ci-après.

© Dunod – La photocopie non autorisée est un délit

➤ Initialisation du LEC

Dans cette phase d'initialisation, le LEC (*LAN Emulation Client*) obtient près du LECS (LAN *Emulation Configuration Server*) l'adresse ATM du LES (*LAN Emulation Server*). Trois méthodes peuvent être utilisées :

– le protocole **ILMI** (*Interim Local Management Interface*), le LEC diffuse une requête de découverte de l'adresse du LECS ;
– une connexion directe à une adresse réservée définie par défaut pour tout le réseau (*Wall Known Address*) ;
– l'utilisation d'un circuit virtuel permanent prédéfini et fixé à l'adresse VPI = 0, VCI = 17 (0/17), cette méthode est aujourd'hui obsolète (LANE V2).

Une fois l'adresse obtenue (protocole ILMI), le LEC établit avec le LECS une connexion temporaire bidirectionnelle appelée : *Configuration Direct VCC*. Le LEC s'enquiert alors, auprès du LECS de l'adresse ATM du LES de l'ELAN qu'il désire rejoindre (figure 13.30, ou *x* représente l'identification de l'ELAN à rejoindre). La connexion avec le LECS est alors rompue.

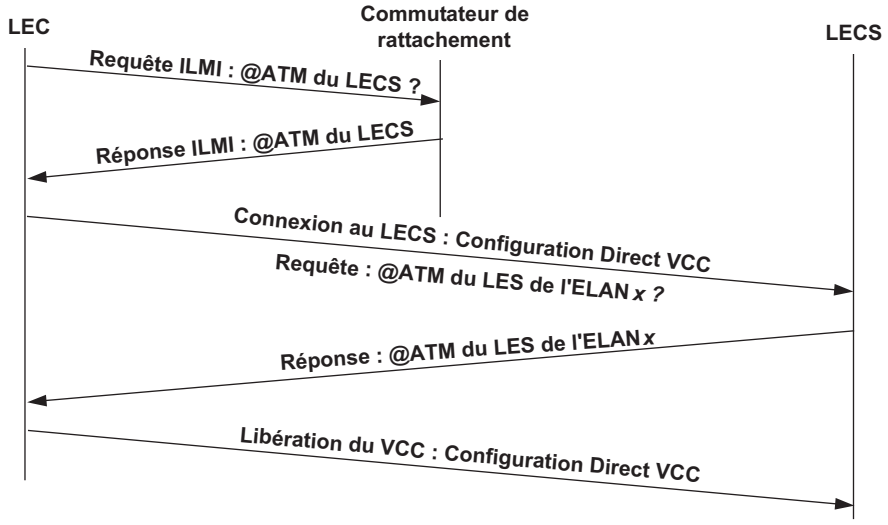

LEC
Commutateur de rattachement
LECS
Requête ILMI : @ATM du LECS ?
Réponse ILMI : @ATM du LECS
Connexion au LECS : Configuration Direct VCC
Requête : @ATM du LES de l'ELAN x ?
Réponse : @ATM du LES de l'ELAN x
Libération du VCC : Configuration Direct VCC

Figure 13.30 Phase de configuration d'un LEC.

➤ Enregistrement auprès du LES

Une fois l'adresse du LES (LAN *Emulation Server*) connue, le LEC établit une connexion bidirectionnelle en point à point (*Control Direct VCC*) avec le LES. Ce dernier lui attribue un identifiant sur deux octets (LEC-ID, *LEC-Identifier*), lui indique le type de réseau émulé (Ethernet, Token Ring) et la taille maximale des trames de données. Le LEC s'enregistre alors auprès du LES en lui fournissant son adresse MAC ou la liste des adresses MAC auxquels il répondra (cas d'un pont par exemple, fonction de LEC proxy). Cet échange est matérialisé par la figure 13.31.

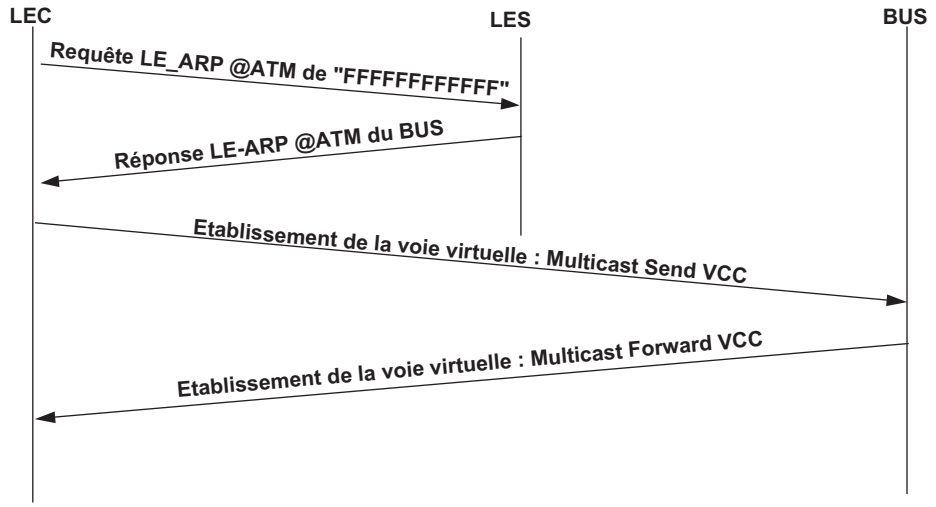

LEC
LES
BUS
Requête LE_ARP @ATM de "FFFFFFFFFFFF"
Réponse LE-ARP @ATM du BUS
Etablissement de la voie virtuelle : Multicast Send VCC
Etablissement de la voie virtuelle : Multicast Forward VCC

Figure 13.31 Enregistrement auprès du LES.

Le LES ouvre une connexion unidirectionnelle multipoint à point avec le LEC (*Control Distribute VCC*). Le LEC n'est pas obligé d'accepter cette connexion (connexion optionnelle).

➤ Connexion au BUS

Pour se connecter au serveur de diffusion (**BUS**, *Broadcast Unknown Server*) le LEC doit auparavant obtenir son adresse auprès du LES. Le LEC émet, vers le LES, une requête LE-ARP (LAN *Emulation* ARP) pour l'adresse de diffusion « FFFFFFFFFFFF ». L'adresse ATM du BUS obtenue, le LEC ouvre une connexion point à point bidirectionnelle avec le BUS (*Multicast Send VCC*), le BUS en retour ouvre une connexion unidirectionnelle en point à multipoint avec le LEC (*Multicast Forward VCC* ou *Multicast Distribute VCC*). Ce processus est représenté figure 13.32.

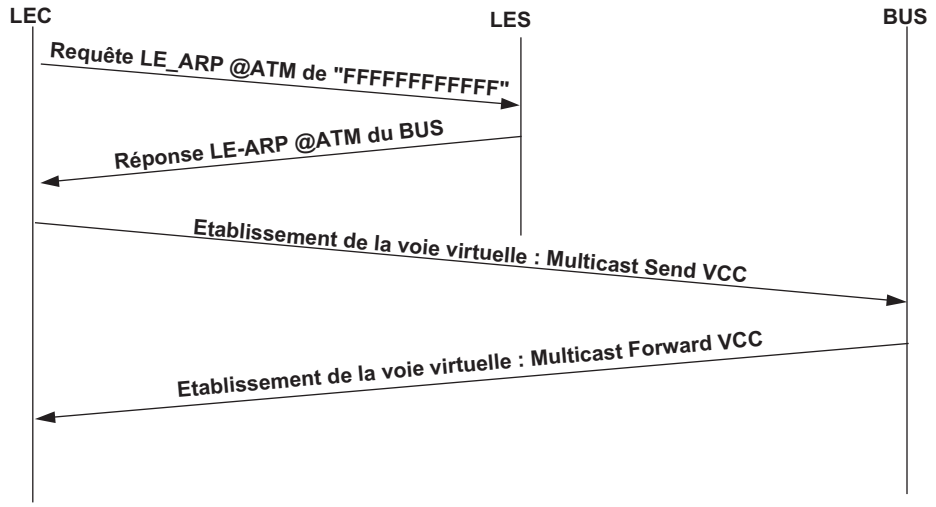

LEC
LES
BUS
Requête LE_ARP @ATM de "FFFFFFFFFFFF"
Réponse LE-ARP @ATM du BUS
Etablissement de la voie virtuelle : Multicast Send VCC
Etablissement de la voie virtuelle : Multicast Forward VCC

Figure 13.32 Connexion du LEC au BUS.

© Dunod – La photocopie non autorisée est un délit

➤ Synthèse des VCC ouverts

La figure 13.33 récapitule toutes les connexions ouvertes durant les différentes phases d'adhésion d'un LEC à un ELAN

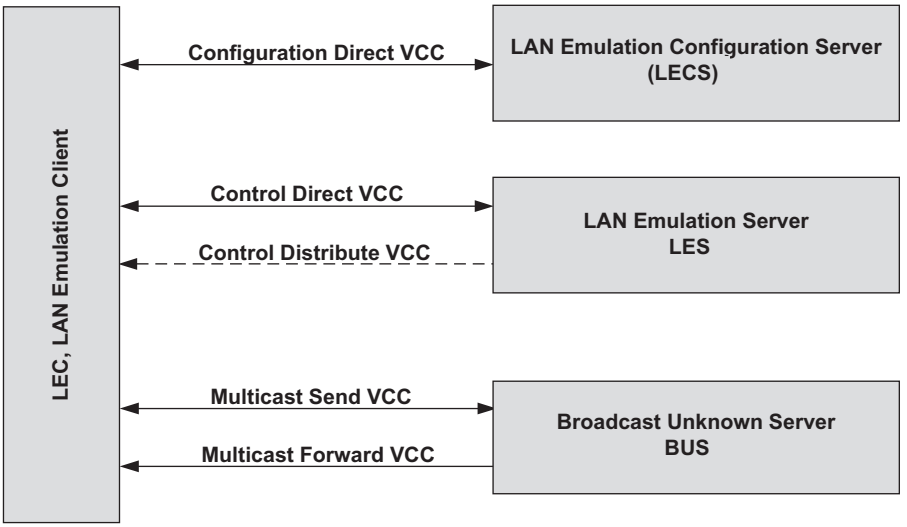


Figure 13.33 Liens entre le LEC et les différents serveurs de l'ELAN.

L'adhésion d'un LEC à un ELAN engendre l'établissement de cinq VCC :

– *Configuration Direct VCC*, connexion bidirectionnelle ouverte par le LEC avec le LECS pour obtenir l'adresse de son LES. Cette connexion est rompue dès que le renseignement est obtenu ;
– *Control Direct VCC*, connexion bidirectionnelle en point à point avec le LES, est utilisé par le protocole LE-ARP ;
– *Control Distribute VCC*, connexion unidirectionnelle en point à multipoint entre le LES et le LEC, ce circuit est utilisé par le LES pour diffuser vers les LEC un message de recherche d'adresse ATM lorsque l'adresse demandée n'est pas dans le cache LE-ARP du LES. Cette connexion est optionnelle, le LEC peut la refuser ;
– *Multicast Send VCC*, connexion bidirectionnelle point à point entre le LEC et le BUS. Cette connexion est utilisée par le LEC pour transmettre un message de diffusion au BUS, celui-ci le diffuse alors sur le *Multicast Forward VCC*. De même, une requête LE-ARP non satisfaite par le LES sera transmise au BUS sur ce circuit ;
– *Multicast Forward VCC*, connexion unidirectionnelle en point à multipoint utilisée par le BUS pour diffuser des messages.

Résolution d'adresses IP/MAC sur un ELAN

Dans un réseau local traditionnel, les stations doivent, avant de communiquer, établir la mise en relation de l'adresse IP et de l'adresse MAC de leur correspondant distant. Cette mise en relation est réalisée par le protocole ARP de TCP/IP. La station ignorant l'existence du réseau ATM, il est nécessaire d'instaurer un mécanisme similaire : la station source émet une requête

ARP et attend une réponse ARP. Les échanges protocolaires de cette résolution d'adresses sont représentés figure 13.34.

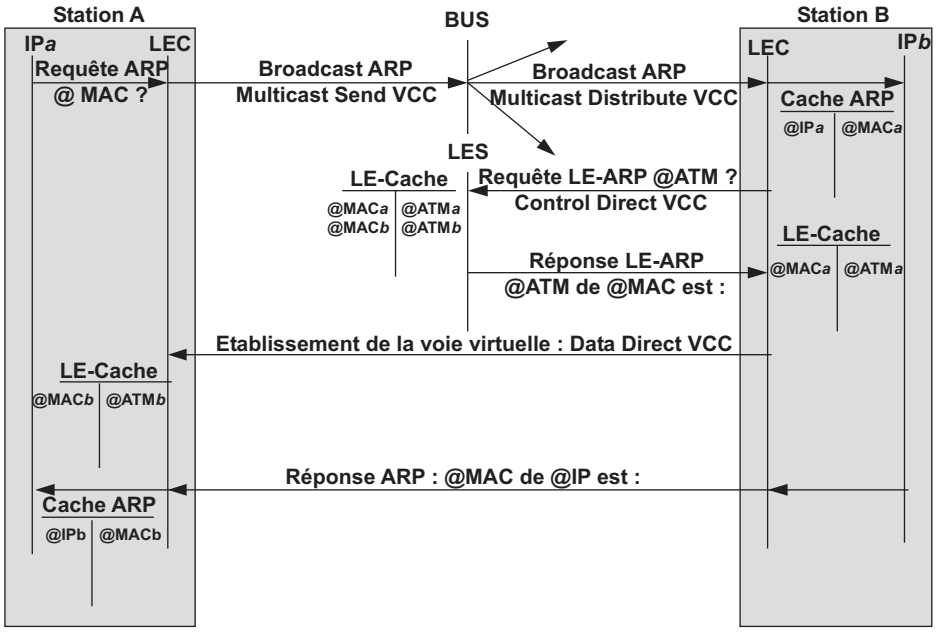


Figure 13.34 Résolution d'adresses IP.

La station source émet sa requête ARP, s'agissant d'un broadcast le LEC transmet celle-ci au BUS sur la connexion *Multicast Send VCC*. Le BUS diffuse la requête sur la connexion qu'il entretient avec tous les LEC en service (*Multicast Distribute VCC*). La station destinataire qui reconnaît son adresse IP, met à jour son cache ARP (@IP/@MAC) et effectue une résolution d'adresses ATM pour répondre à la station source (il n'en connaît que l'adresse IP et l'adresse MAC contenues dans le message ARP). Pour cela, il émet une requête LE-ARP au LES sur la connexion LEC/LES (*Control Direct VCC*), le LES consulte sa table LE-ARP (cache LE-ARP) et retourne l'adresse ATM recherchée. La station destinataire établit alors une connexion bidirectionnelle avec la station source (*Data Direct VCC*) et transmet la réponse ARP. Les deux stations peuvent alors communiquer directement.

Imaginons la complexité du système, le trafic induit et ses conséquences sur les performances générales du réseau, quand la station source doit se connecter à un serveur de noms pour obtenir l'adresse IP de la machine cible !

LAN Emulation 2

LAN Emulation préserve les applications existantes. Indépendant des protocoles il fonctionne avec NetBIOS, IXP, IP... Cependant, la première version de LAN *Emulation* présente quelques inconvénients majeurs dont le principal est la non-réplication des différents serveurs. Ce défaut est corrigé avec la version 2.

LAN *Emulation 1* ne gère pas la qualité de service, seul, le trafic de type UBR (*Unspecified Bit Rate*) est offert. LAN *Emulation 2* gère le trafic UBR et le trafic ABR (*Avalaible Bit Rate*).

© Dunod – La photocopie non autorisée est un délit

De plus, il introduit, pour lutter contre la congestion, le mécanisme dit du rejet prématuré de paquet (**EPD**, *Early Packet Discard*).

Dans un réseau émulé, la perte d'une cellule (par exemple, une cellule détruite par un nœud en état de congestion) conduit à la retransmission de tout le datagramme (une trame Ethernet correspond à 32 cellules), ce qui ne fait qu'aggraver la congestion. Suite à une perte de cellule due à un état de congestion ou à une erreur sur l'en-tête, le mécanisme EPD élimine toutes les cellules de ce datagramme sauf la dernière. La dernière cellule sera transmise à l'utilisateur afin de délimiter la première cellule du datagramme suivant. Cette méthode améliore la gestion et la prévention de la congestion par l'élimination de nombreuses cellules inutiles.

13.3.4 Interconnexion de réseaux LANE (MPOA)

Principe

MPOA (*MultiProtocol Over ATM*) a été défini par l'ATM Forum pour permettre aux protocoles de niveau 3[4] comme IP, IPX, Appletalk, etc., d'exploiter les possibilités d'ATM (débit, qualité de service...). MPOA autorise une communication directe entre deux systèmes d'extrémité n'appartenant pas au même réseau logique virtuel (VLAN ou subnet différent) sans passer par un routeur. La figure 13.35 illustre les techniques LANE et MPOA.

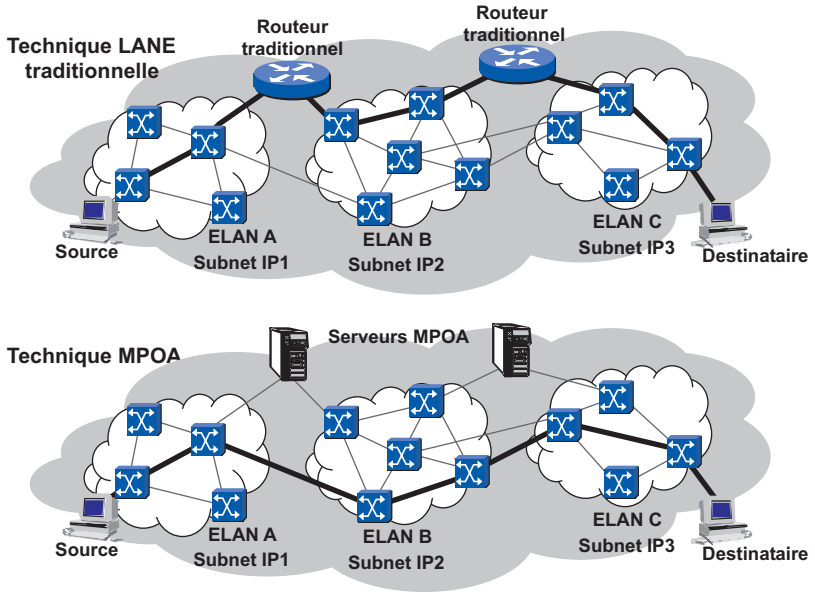


Figure 13.35 Principe de MPOA.

Dans la technique LANE traditionnelle, tout le flux de données transite par le routeur. Tandis que, dans l'approche MPOA, une fois le flux identifié (couple @IP source/@IP destination), un circuit virtuel commuté (VCC) est établi entre les deux équipements d'extrémité.

4. Actuellement MPOA ne fonctionne qu'avec IP du DoD.

MPOA exploite la technologie LANE (LAN *Emulation*) et pallie ses limites en offrant une émulation transparente des protocoles réseaux s'exécutant au-dessus d'ATM. MPOA assure une connectivité de niveau 3 de bout en bout entre les systèmes d'extrémité, qu'ils soient directement raccordés à une infrastructure ATM ou à un sous-système de technologie antérieure.

L'avantage primordial de l'approche MPOA réside dans le fait que chaque système intégrant une interface MPOA peut établir des connexions ATM directes (sans intermédiaire) de type unicast, multicast et broadcast.

Fonctionnement de MPOA

➤ Architecture de MPOA

À l'instar de LANE, MPOA fonctionne selon le modèle client/serveur. Il comporte deux éléments :

– le client (*MPOA client*, **MPC**), élément logiciel résident dans l'équipement terminal ou le commutateur de bordure[5] (*edge device*) raccordé à ATM. Le client MPC inclut les services de la RFC 1 483 pour assurer un transfert de données hors LEC ;

– le serveur (*MPOA server*, **MPS**) est une extension logicielle résidente dans les routeurs interréseaux.

MPOA ne fonctionne que sur LANE2. La communication entre MPC (MPOA *Client*) et MPS (MPOA *Serveur*) s'effectue via les LAN Emulation Clients (LEC). La communication entre serveurs MPOA (MPS) utilise le protocole NHRP (*Next Hop Routing Protocol*). La figure 13.36 schématise cette architecture.

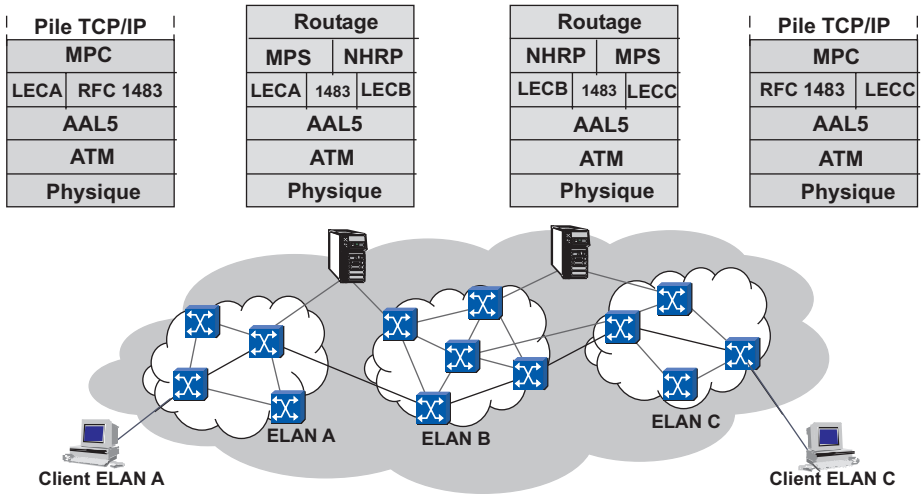


Figure 13.36 Architecture d'une interconnexion MPOA.

5. C'est par exemple le cas d'un commutateur Ethernet disposant d'un raccordement ATM.

© Dunod – La photocopie non autorisée est un délit

➤ Principe de fonctionnement de MPOA

Dans la technique LANE (LAN *Emulation*) traditionnelle, la communication entre deux stations appartenant à deux ELAN (*Emulated* LAN) différents s'établit en deux temps. La station source établit un circuit virtuel commuté (VCC) avec le routeur et ce dernier procède de même avec la station destinataire. Toutes les cellules ATM sont alors acheminées vers le routeur et réassemblées pour reconstituer le datagramme IP d'origine. Ce dernier est alors traité selon un protocole de routage classique puis de nouveau segmenté en cellules pour être émis sur le CV routeur/station destination. Ce processus ne peut que constituer un goulet d'étranglement incompatible avec les débits source et destination offerts par les réseaux ATM.

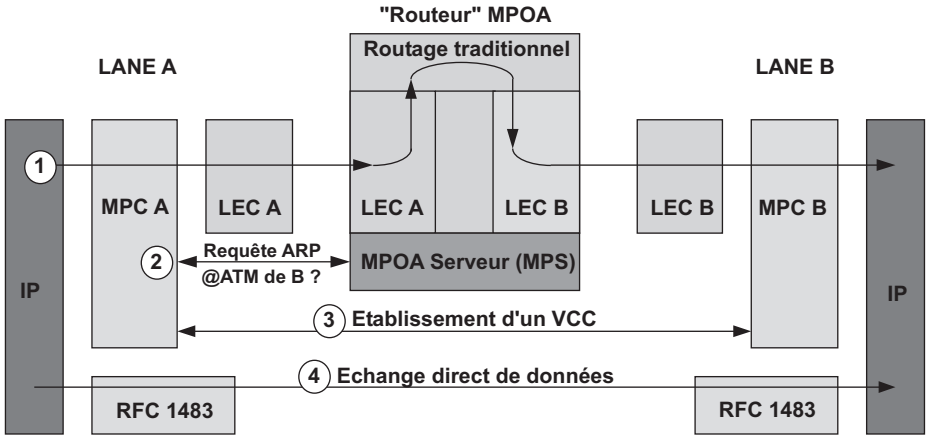


Figure 13.37 Principe de fonctionnement de MPOA.

Dans l'architecture MPOA (figure 13.37), la communication s'établit d'abord normalement selon le scénario décrit ci-dessus, puis :

– Le client MPOA (MPC) de la machine source identifie un flux (succession de datagrammes vers une même destination), il consulte alors sa table en mémoire cache pour vérifier s'il existe déjà un circuit virtuel vers cette destination. Si ce n'est le cas, il adresse une requête au MPS (MPOA *Server*) pour obtenir l'adresse ATM de la destination.

– Si le MPS ne dispose pas de cette adresse dans ses tables, il interroge les autres MPS selon une procédure NHRP pour résoudre cette adresse ATM.

– Ayant obtenu l'adresse ATM du destinataire, le MPC source établit un circuit virtuel commuté (VCC) directement avec ce dernier.

– Le flux IP est alors envoyé directement sur ce circuit selon l'encapsulation RFC 1483 appelée aussi VC *Based Multiplexing*.

13.4 CONCLUSION

Les réseaux métropolitains traditionnels ne sont plus en adéquation avec les débits des composantes locales des réseaux d'entreprises. ATM était prometteur, surtout en terme de qualité de service, mais la complexité de LAN *Emulation* ne lui a pas permis de s'imposer. La voie est ainsi largement ouverte au 10 Gigabit Ethernet.

EXERCICES

Exercice 13.1 FDDI et Token Ring

Comparez les caractéristiques physiques et fonctionnelles des réseaux Token Ring et FDDI

Exercice 13.2 Données de la classe Isochrone

Est-il envisageable d'émettre des données Isochrone sur un réseau FDDI-1

Exercice 13.3 L'acquittement dans FDDI

Dans FDDI le champ FS comporte les informations en relation avec l'indication de détection d'erreur, d'adresse reconnue et de trame recopiée. Donnez la structure de ce champ lors de l'envoi d'une trame multicast alors que trois stations ont reconnu leur adresse mais seulement deux ont correctement recopié la trame.

Exercice 13.4 Rotation des données sur le réseau FDDI

Supposons un réseau FDDI ne comportant que 4 stations. Représenter la circulation des données sur l'anneau en admettant que :

– avant l'échange seul le jeton circule sur l'anneau ;

– la station 1 acquiert le jeton et transmet des données à la station 3 ;

– la station 2 acquiert le jeton et transmet des données à la station 4.

On considérera que la trame est très petite devant la taille de l'anneau.

Exercice 13.5 État des compteurs dans DQDB

Une station a le compteur RQ positionné à 5 et le compteur CD positionné à 2, elle désire émettre des données. Aucune nouvelle requête en amont n'étant formulée combien de slots vides devra-t-elle décompter avant de pouvoir émettre ses données ?

© Dunod – La photocopie non autorisée est un délit

Chapitre **14**

Interconnexion des réseaux

14.1 GÉNÉRALITÉS

14.1.1 Définition

Le déploiement des réseaux d'établissement a permis le traitement local des informations. Cependant, pour assurer la cohérence du système d'information de l'entreprise, il s'avère nécessaire d'assurer l'échange d'information entre ses différentes composantes. Tel est l'objet de l'interconnexion des réseaux. Fonctionnellement, l'interconnexion consiste à mettre en relation, indépendamment de la distance qui les sépare et des protocoles qu'elles utilisent, des machines appartenant à des réseaux physiquement distincts.

Physiquement, elle se réduit à la mise en relation de deux réseaux via un organe, appelé relais dans la terminologie OSI. Le relais peut n'être qu'un simple élément physique mais aussi un réseau (figure 14.1).

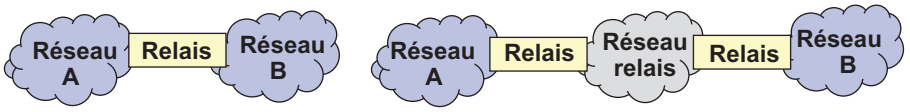


Figure 14.1 Principe de l'interconnexion des réseaux.

14.1.2 Problématique de l'interconnexion

La mise en relation d'un système A avec un système B peut se réaliser très simplement si A, B et le relais utilisent les mêmes protocoles, comme par exemple l'interconnexion de deux réseaux locaux utilisant TCP/IP via un réseau IP. Cependant, dans la plupart des cas, le protocole du réseau relais est différent du protocole local, par exemple l'interconnexion de deux réseaux locaux TCP/IP via un réseau de transport X.25, FR ou ATM. L'hétérogénéité peut aussi être de bout en bout, quand les deux éléments à raccorder mettent en œuvre des tech-

nologies différentes. Dans ce dernier cas, pour assurer l'interfonctionnement des systèmes, une unité d'interfonctionnement (**UIF**) réalise les adaptations nécessaires. Trois techniques peuvent alors être utilisées : la conversion de service, la conversion de protocole et l'encapsulation.

14.1.3 Notions de conversion de service et de protocole

Dans la conversion de service (figure 14.2), le relais reçoit les messages selon le format B, il assure la transposition de l'unité de service SDU(B) en une unité de service SDU(C). Cette technique est utilisable lorsque les protocoles à mettre en relation sont différents mais compatibles. C'est le cas, par exemple, du passage d'un réseau 802.3 10 base 5 à un réseau 802.3 10 base T. L'UIF intervient alors au niveau physique (sous-couche **PMD**, *Physical Medium Dependant*).

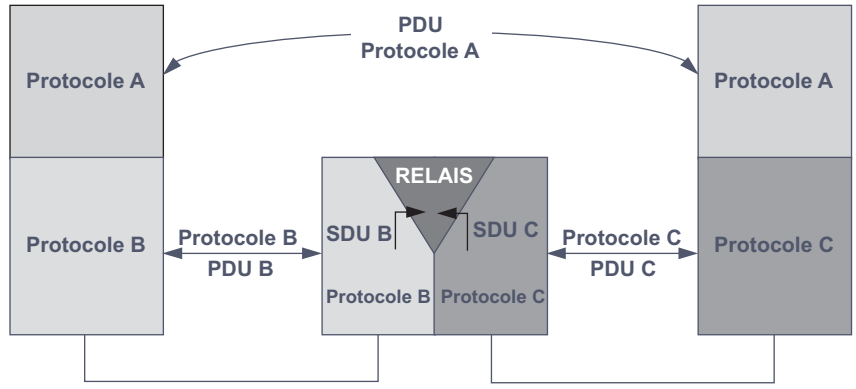


Figure 14.2 La conversion de service.

La conversion de protocole (figure 14.3) intervient lorsque les protocoles d'extrémité sont différents et incompatibles. C'est, par exemple, le cas lors de l'interconnexion d'un réseau de type Ethernet et d'un réseau de type Token Ring, l'UIF intervient ici au niveau MAC.

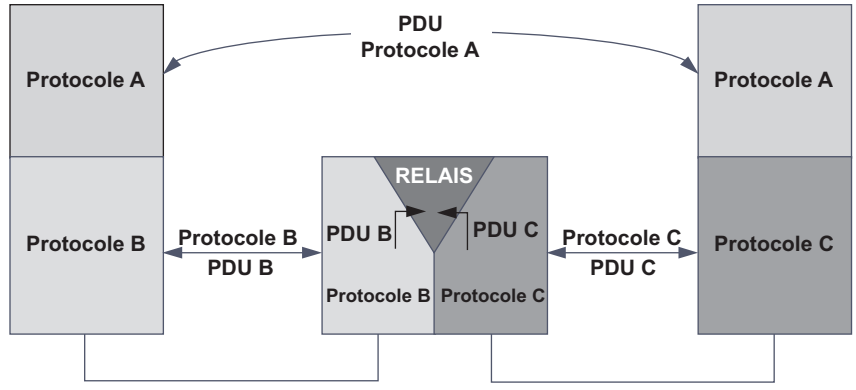


Figure 14.3 La conversion de protocole

La différence entre les deux méthodes est toute théorique et transparente à l'utilisateur.

14.1.4 L'encapsulation ou *tunneling*

La conversion de protocole est irréversible. En effet, si on interconnecte deux réseaux IP via par exemple un réseau X.25, il est aisé, à partir des informations d'en-tête du datagramme IP de confectionner un en-tête X.25, mais il est totalement impossible à partir des données d'en-tête X.25 de reconstruire le datagramme d'origine. Pour disposer des informations nécessaires à la reconstruction du datagramme d'origine, il suffirait d'insérer un sous-champ entre l'en-tête du nouveau protocole et les données à transporter. Cette méthode serait lourde, il est préférable de transporter, dans le champ X.25, le datagramme complet IP. Le travail des UIF s'en trouve facilité. Ce mécanisme se nomme encapsulation de données. On parle aussi de *tunneling*, car on a réalisé un « tunnel » X.25 qui transporte des données IP. L'encapsulation de données est illustrée par la figure 14.4.

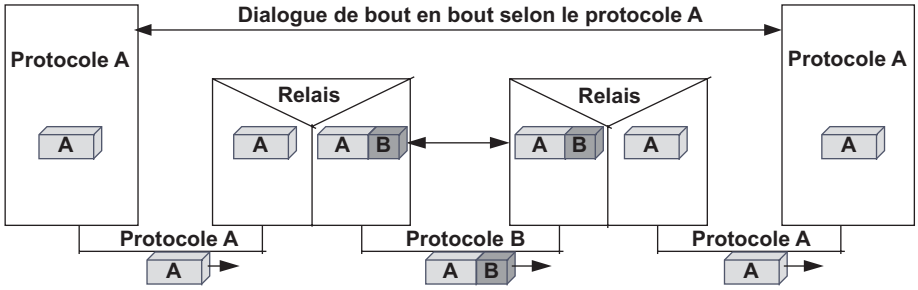


Figure 14.4 L'encapsulation de données.

Dans le schéma de la figure 14.4, les PDU du protocole A, issues de l'un des systèmes, sont encapsulées dans des PDU du protocole B par le premier relais. Les données sont transférées en mode transparent par le réseau qui considère la PDU A comme des données. Le relais final exécute l'opération inverse, la PDU du protocole A est restituée.

L'encapsulation est utilisée chaque fois que le protocole du réseau intermédiaire (relais) est incompatible avec celui des réseaux d'extrémités.

14.1.5 Les différents types de relais

Selon le niveau où se réalise l'interconnexion, l'ISO distingue quatre types de relais (figure 14.5) :

– les répéteurs, organes d'interconnexion locaux, ils agissent au niveau 1 du modèle de référence ;

– les ponts (*bridges*) interviennent au niveau 2 ;

– les routeurs[1] sont des éléments d'interconnexion de niveau 3 ;

– au-dessus, on parle de passerelles. Cependant, l'usage désigne une interconnexion de

1. En principe, il conviendrait de réserver le terme de routeur à l'interconnexion de réseaux dont les espaces d'adressage sont homogènes et d'utiliser le terme de passerelle interréseau lorsque les espaces d'adressage des réseaux interconnectés sont différents. Cependant, le langage courant utilise le terme de routeur dans les deux cas. Nous nous conformerons à cet usage.

© Dunod – La photocopie non autorisée est un délit

niveau 4 comme un adossement de transport. L'adossement de transport n'est pas conforme au modèle de référence la couche 4 n'étant plus de bout en bout.

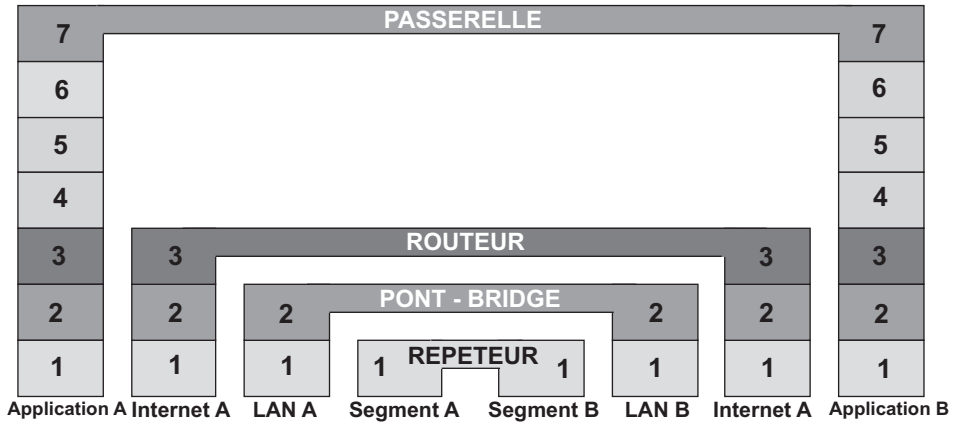


Figure 14.5 Les organes d'interconnexion selon l'ISO

Généralement les passerelles agissent au niveau applicatif, elles mettent en relation des applications de même nature mais d'architecture différente ; c'est, par exemple, le cas d'une interconnexion d'une messagerie **SMTP** (*Simple Mail Transfer Protocol*) du monde TCP/IP avec une messagerie X.400 du monde ISO.

14.2 LES RÉPÉTEURS

Les répéteurs réalisent une connexion physique entre deux segments d'un même réseau logique (figure 14.6). Agissant au niveau physique, les réseaux interconnectés doivent être homogènes. Un répéteur ne fait que retransmettre d'un côté les bits reçus sur l'autre, il agit par diffusion.

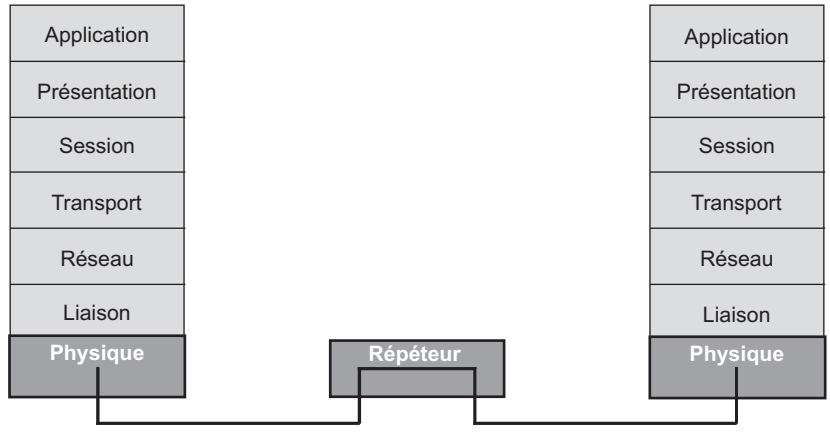


Figure 14.6 Situation des répéteurs dans le modèle OSI.

De ce fait, il ne peut que réaliser la prolongation ou l'adaptation d'un support et non pas une interconnexion, au sens fonctionnel, de deux réseaux. Ils sont utilisés pour réaliser l'adapta-

tion des supports (passage coaxial à la fibre optique, par exemple) ou pour accroître la portée géographique d'un réseau (régénération du signal et récupération d'horloge, figure 14.7). L'utilisation de répéteurs est sans incidence sur les protocoles transportés. Cependant, augmentant la portée du réseau, il peut être nécessaire de modifier les temporisations.

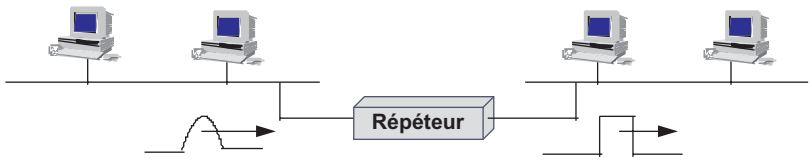


Figure 14.7 Fonction de régénération de signaux des répéteurs.

Les répéteurs peuvent aussi être utilisés pour réaliser l'isolation galvanique de deux segments de réseau alimentés par des réseaux électriques différents ou reliés à des terres dont l'équipotentialité n'a pas été réalisée (interconnexion de réseaux situés dans des bâtiments différents ou alimentés par des réseaux courant fort[2] différents).

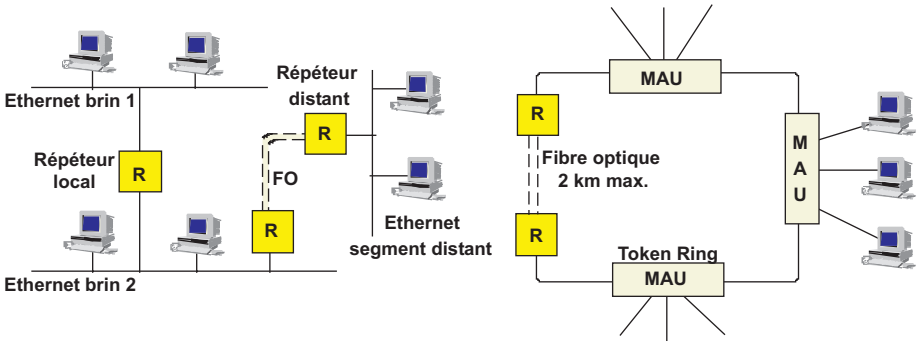


Figure 14.8 L'interconnexion par des répéteurs.

La figure 14.8 situe l'utilisation de répéteurs dans les réseaux de type Ethernet et Token Ring.

14.3 LES PONTS

14.3.1 Généralités

Les ponts ou *bridges* sont des éléments d'interconnexion de niveau 2. Ils permettent d'interconnecter deux ou plusieurs réseaux (ponts multiports) dont les couches physiques sont dissemblables (figure 14.9). Les ponts sont transparents aux protocoles de niveau supérieur.

Les ponts assurent des fonctions d'adaptation de débit ou de support entre réseaux semblables (Ethernet/Ethernet ou Token Ring/Token Ring) ou dissemblables (Ethernet/Token Ring). Agissant au niveau 2 du modèle de référence, les ponts ont accès à l'adresse MAC. De ce fait, ils peuvent acheminer les trames, en fonction de l'adresse MAC, réalisant ainsi un

2. On appelle courant fort la distribution de l'énergie électrique et par opposition courant faible les réseaux filaires téléphoniques et informatiques.

© Dunod – La photocopie non autorisée est un délit

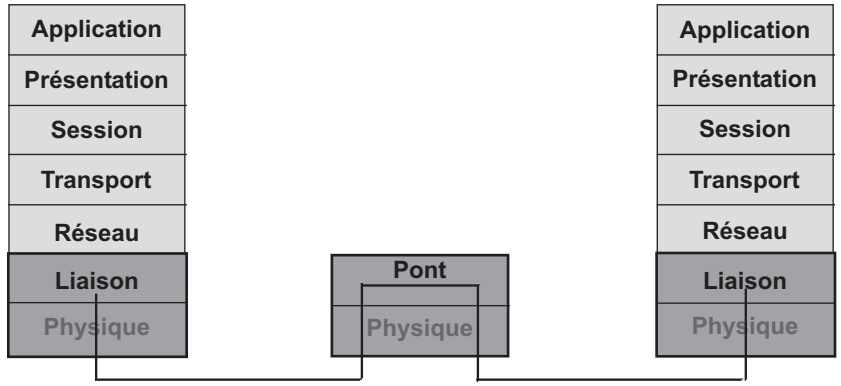


Figure 14.9 Situation des ponts dans le modèle OSI.

« routage de niveau 2 » (figure 14.10). Les ponts ne peuvent interconnecter que des réseaux dont l'espace d'adressage est homogène. Les réseaux interconnectés constituent un seul et unique réseau logique.

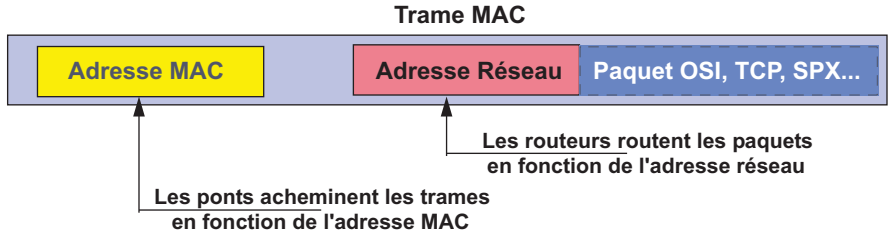


Figure 14.10 Fonction de filtrage et d'acheminement des ponts.

14.3.2 Les différents types de ponts

Les ponts sont caractérisés par le mode d'établissement des tables d'acheminement et par la distance qui sépare les réseaux interconnectés. On distingue :

- les ponts simples, sans fonction d'acheminement, qui diffusent toutes les trames reçues sur tous les ports (sauf le port d'arrivée), ces ponts ne sont plus utilisés, ce sont de simples répéteurs multiport ;
- les ponts simples, avec fonction d'acheminement, ces derniers dirigent les trames selon une table d'acheminement introduite à la configuration du pont (pontage statique) ;
- les ponts transparents (**TB**, *Transparent Bridging*) ou ponts à apprentissage (*learning bridge*), ces ponts construisent dynamiquement la table d'acheminement et la maintiennent à jour ;
- les ponts à routage par la source, ou contrôlé par l'émetteur (*source routing*), dans ces ponts, la route suivie par la trame est indiquée dans la trame elle-même. Préalablement à l'envoi de données, la source émet une trame de découverte de route vers le destinataire, cette route est mémorisée et indiquée dans tout message vers cette même destination. D'origine IBM, le routage par la source est utilisé dans l'interconnexion des réseaux Token Ring et FDDI ;
- enfin, on distingue les ponts locaux des ponts distants (*remote bridge*). Les ponts distants interconnectent des réseaux locaux via une liaison spécialisée ou un réseau de transport

(figure 14.11). Ils doivent assurer des fonctions d'adaptation de protocole entre le protocole local et le protocole du lien d'interconnexion (X.25, Frame Relay, ATM, PPP...). Ces ponts sont généralement désignés sous le terme de pont à encapsulation.

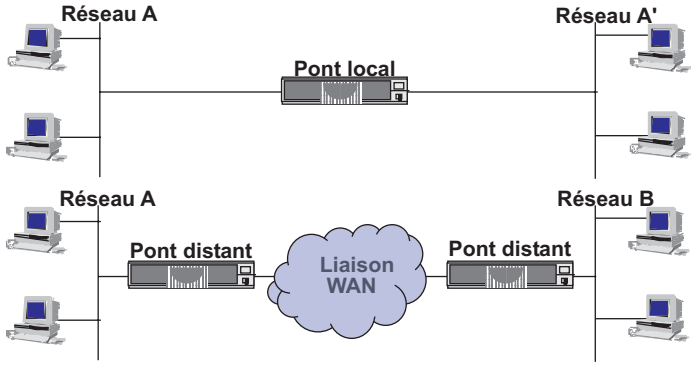


Figure 14.11 Pont local et pont distant

14.3.3 Les ponts transparents

À l'instar des commutateurs[3], les ponts établissent dynamiquement, par écoute du trafic sur chacun de ses ports, une table d'acheminement (**FDB**, *Forwarding Data Base*). La FDB mémorise le couple port de réception/adresse MAC source (figure 14.12). À réception d'une trame, le pont consulte la table d'acheminement, s'il possède une entrée dans la table pour l'adresse destination, il achemine la trame reçue sur le seul port où est localisé le destinataire. Les trames à destination d'une adresse non inscrite dans la table et celles de diffusion sont répétées sur tous les ports, sauf le port de réception.

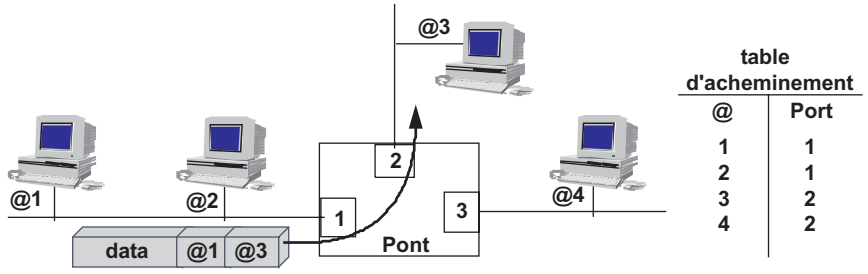


Figure 14.12 Principe d'acheminement des ponts.

À chaque entrée dans la table est associée une temporisation, à l'échéance du *timer*, l'entrée est effacée. À chaque réception d'une trame de même origine, le timer est réinitialisé. Ce procédé autorise la mobilité et évite l'engorgement des tables. Par défaut, la valeur de la temporisation est fixée à 5 mn, elle est paramétrable de 10 s à 11 jours. En principe une table peut contenir jusqu'à 1 024 entrées, ce nombre correspond au nombre maximal de stations actives sur un réseau Ethernet

3. Il conviendrait plutôt d'écrire : « À l'instar des ponts, les commutateurs... ». Rappelons que nous avons défini section 12.7, les commutateurs comme étant des ponts performants.

© Dunod – La photocopie non autorisée est un délit

La table peut être modifiée par l'administrateur, il est alors possible de réaliser des filtres (filtrage statique). En associant des adresses sans limite d'âge à un port on interdit la mobilité des stations. On peut de même, en fonction d'une adresse source ou destination, interdire l'acheminement vers tel ou tel port. La figure 14.13 illustre le traitement réalisé par un pont lors de la réception d'une trame.

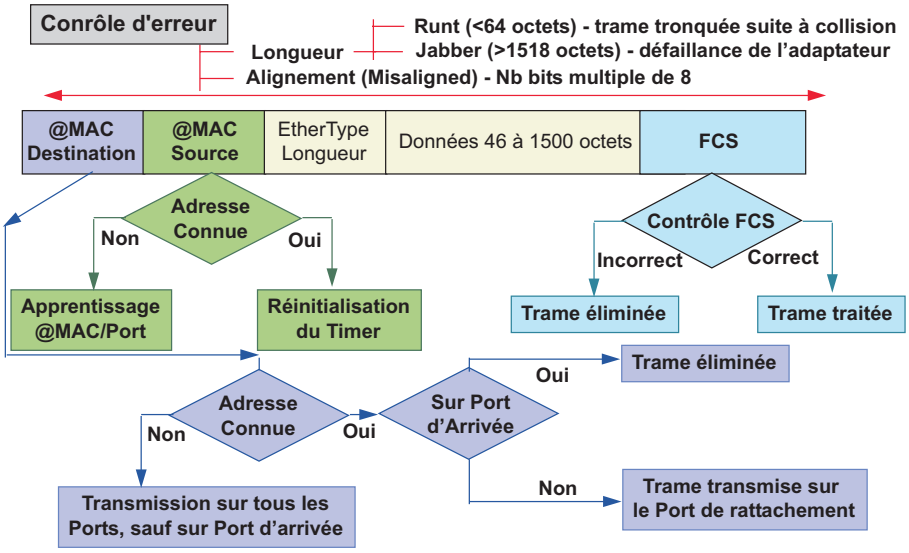


Figure 14.13 Traitement des trames 802.3 dans un pont.

La fonction d'acheminement des ponts permet d'isoler chaque brin du trafic existant sur un autre brin. Cette faculté associée à la non-retransmission des trames erronées (erreurs de FCS, trame incomplète...) permet, dans les réseaux de type Ethernet, de découper un réseau physique en plusieurs sous-réseaux logiques, dits réseaux de collisions. Une collision sur un brin est invisible sur un autre. L'architecture adoptée est généralement du type *backbone* (réseau fédérateur). Dans ce type d'architecture d'interconnexion (figure 14.14), seul le trafic interservice transite sur le réseau backbone.

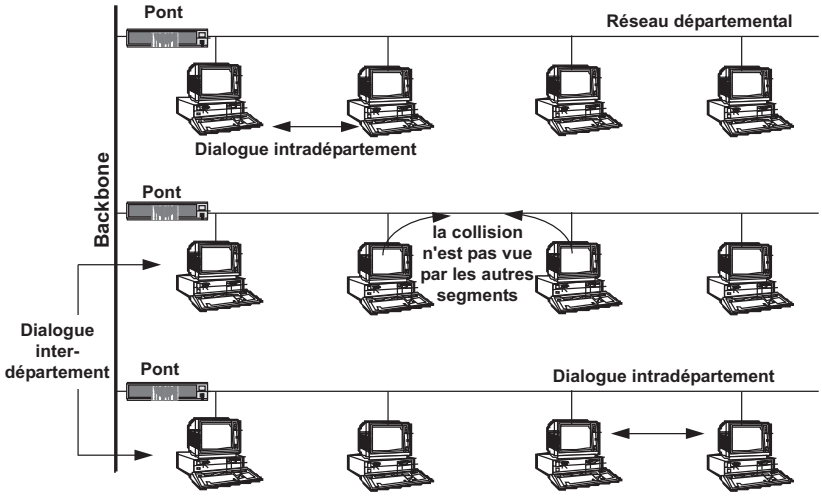


Figure 14.14 Architecture d'un réseau *backbone*.

Le pont est, vis-à-vis du trafic applicatif sur le réseau, un élément passif. Il n'a donc en principe nul besoin d'une adresse MAC. Cependant, pour des raisons d'administration, à chaque interface MAC du pont est associée une adresse MAC.

14.3.4 Le *Spanning Tree Protocol* (STP) ou arbre recouvrant

Généralités

Les facultés d'autoconfiguration des ponts transparents en ont fait l'un des éléments majeurs de l'interconnexion locale des grands réseaux. La sécurisation du réseau a fait apparaître la nécessité de duplexer les organes d'interconnexion (figure 14.15).

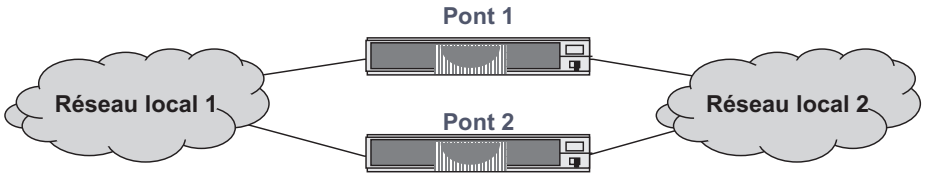


Figure 14.15 Interconnexion redondante.

Cependant, la mise en parallèle de ponts transparents volontaire, par mesure de sécurité, ou par erreur, dans un réseau complexe, engendre un phénomène de bouclage qui conduit à l'effondrement du réseau. Ce phénomène est illustré par la figure 14.16.

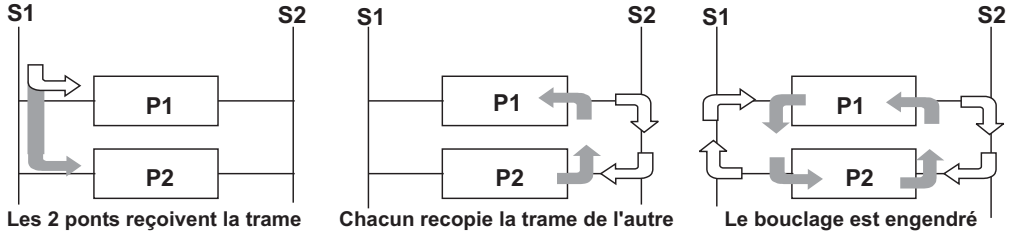


Figure 14.16 Bouclage des trames sur des ponts en parallèle.

La trame émise sur le segment S1 à destination d'une station non encore enregistrée dans les ponts est reçue par les deux ponts (P1 et P2), elle est retransmise sur le segment S2, la trame émise par le pont 1 sur le segment 2 est reçue par le pont 2, tandis que celle émise par le pont 2 est recopiée par le pont 1. Chacun recopie alors la trame sur le segment 1... Une situation de boucle est engendrée. Développé à l'origine par DEC et normalisé par l'IEEE (IEEE 802.1D), l'algorithme du *spanning tree* (**STP**, *Spanning Tree Protocol*) est un protocole d'apprentissage de la topologie du réseau dont le but est d'éliminer les boucles en désactivant les ports des ponts qui engendrent ces boucles.

Le principe en est relativement simple, il s'agit de construire un graphe en arbre. À partir d'un pont élu, désigné pont racine (*bridge root*), l'algorithme du *spanning tree* détermine le chemin le plus court en éliminant les risques de bouclage. Les ponts en boucle sont déclarés pont *backup* et mis en sommeil (figure 14.17).

© Dunod – La photocopie non autorisée est un délit

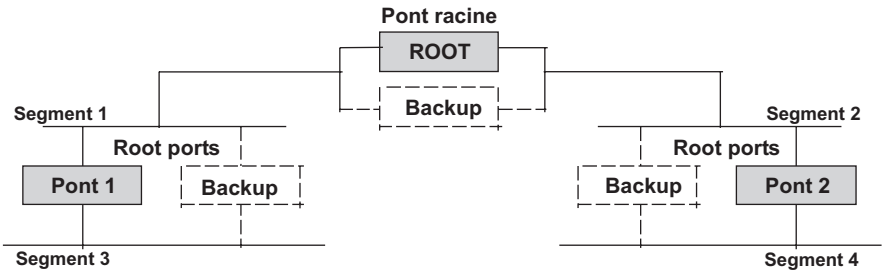


Figure 14.17 Exemple de configuration du *Spanning Tree Protocol*.

L'algorithme du spanning tree

Pour construire l'arbre recouvrant (*spanning tree*) les ponts s'échangent des messages de diffusion (**BPDU**, *Bridge Protocol Data Unit*). Le *spanning tree* utilise deux types de messages, les messages de configuration (figure 14.18) et les messages d'indication de changement de topologie.

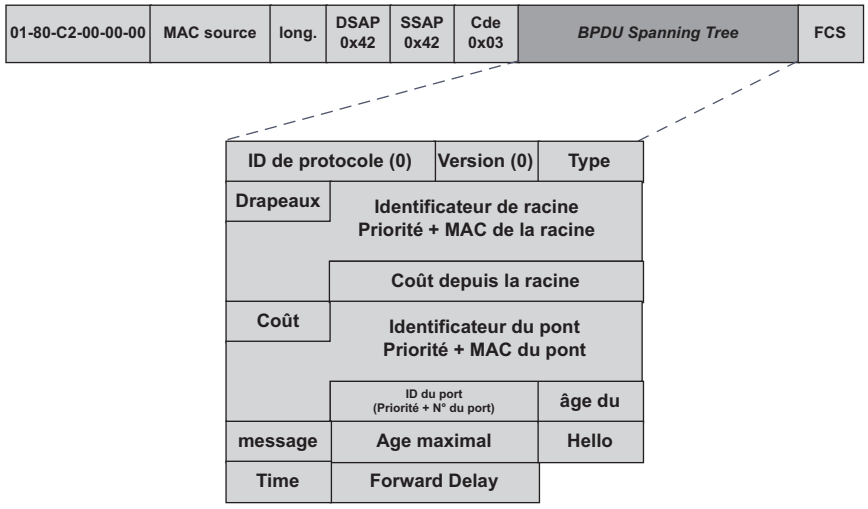


Figure 14.18 La BPDU de configuration.

Le message de configuration (BPDU de configuration) utilise l'encapsulation IEEE 802.2 LLC1 (*Logical Link Control* mode datagramme) avec un SAP de 0x42 et une adresse MAC (*Medium Access Control*) destination de diffusion 01-80-C2-00-00-00 en Ethernet et 03-00-00-00-80-00 en Token Ring. Les champs identification du protocole, *Type* sur 2 octets, et *Version* (1 octet), non utilisés, doivent toujours être mis à 0. Le champ suivant sur 1 octet distingue un message de configuration (0), d'un message d'information de topologie (128).

Chaque pont possède un identificateur (**ID**, *bridge IDentifier*) construit à partir d'un indicateur de priorité (2 octets de poids fort du champ) et de l'adresse MAC du pont. Le champ priorité est fixé à 0x8000 par défaut. Sa valeur peut être modifiée par l'administrateur (0 à 0xFFFF). Plus ce nombre est faible, plus la priorité est élevée. Le pont racine élu est le pont de plus petit ID, à priorité égale c'est celui de plus petite adresse MAC. Au démarrage, chaque

pont émet une BPDU le signalant comme pont racine. Tout pont qui reçoit une BPDU avec un ID inférieur au sien, cesse ses émissions et rediffuse les trames reçues. À la fin du processus, seul le pont racine continue à émettre son identifiant. Il est élu pont racine.

Le port, par lequel, un pont reçoit en premier la trame d'identification du pont racine est appelé « *root port* ». Pour déterminer l'arbre minimal, chaque pont se voit affecter, par l'administrateur, un coût. Le pont racine émet une trame de diffusion avec un coût nul, chaque pont répète cette trame en incrémentant le coût du sien (*root path cost*). Un pont qui reçoit, sur un port « non-racine », une trame dont le coût, depuis la racine, est inférieur au coût des trames qu'il émet, en déduit qu'il existe, depuis la racine, une route moins chère. Il se met alors en sommeil (pont *backup*). En cas d'égalité entre deux ponts, c'est le pont de plus petit ID qui est élu. L'éventuel pont en boucle sur la racine détermine qu'il est pont backup simplement parce qu'il reçoit des trames identiques sur ses deux ports et que son ID est supérieur. En principe, le coût de traversée des ponts est le même pour tous, la valeur recommandée était « 1 000/Débit en Mbit/s ». L'accroissement des débits a rendu cette valeur obsolète, la recommandation IEEE 802.1p fixe de nouvelle valeur (figure 14.19). Il est possible, en jouant sur les valeurs du niveau de priorité et de coût, de privilégier un chemin par rapport à un autre.

Débit du réseau	Valeurs recommandées	Plages admises
Réseaux IEEE 802.3		
10 Mbit/s	100	50-600
100 Mbit/s	19	10-60
1 Gigabit/s	4	3-10
10 Gigabit/s	2	1-5
Réseaux IEEE 802.5		
4 Mbit/s	250	100-1 000
16 Mbit/s	62	40-400
100 Mbit/s	19	10-60

Figure 14.19 Valeur des coûts recommandée par l'IEEE.

Périodiquement une trame de diffusion est émise, la valeur par défaut du paramètre *Hello Time* est de 2 s, valeur recommandée 20 s. Si un pont *backup* reste plus de cet intervalle de temps sans rien recevoir, il en déduit que le pont, dont il est le backup, est défaillant. Il émet alors une trame de configuration. Cette diffusion de BPDU, sur un lien WAN, peut consommer une partie importante de la bande passante. Aussi, il convient d'éviter de mettre en service le *spanning tree* lorsque les réseaux sont interconnectés via des liens WAN à faible bande passante.

Les informations suivantes sont fixées par la racine, l'âge du message est fixé à 0 et retransmis tel quel par chaque pont. Lorsqu'un pont ne reçoit plus de message, il retransmet le dernier message reçu en incrémentant ce champ du nombre de périodes d'émission (*Hello Time*) depuis la dernière réception. Lorsqu'un message atteint l'âge maximal, il est détruit. La valeur du champ *Forward Delay* correspond au temps maximal entre les différentes étapes de configuration (valeur par défaut 15 s). Tous ces champs sont codés en 1/256 de seconde.

Les ponts transparents peuvent être dans 5 états :

– l'état *Disabled*, dans cet état le pont ne participe à aucune activité, il est inerte ;

© Dunod – La photocopie non autorisée est un délit

– l'état *Listening* correspond à la phase de configuration et de construction de l'arbre recouvrant. Dans cet état, le pont n'accepte, ni ne retransmet les trames utilisateurs ;
– l'état *Learning*, c'est la phase d'apprentissage, le pont met à jour sa base de données d'acheminement. Dans cet état, le pont ne participe toujours pas à la retransmission des trames ;
– l'état *Forwarning*, c'est l'état de fonctionnement normal d'un pont, il participe alors à l'acheminement des trames sur le réseau ;
– enfin, l'état *Blocking*, dans cet état le pont est en sommeil, il n'achemine aucune trame mais participe aux opérations du *spanning tree* et d'administration des ponts.

Conclusion

L'algorithme du *Spanning Tree Protocol* utilise une adresse de diffusion. En cas de système multiconstructeur, il est important de vérifier que les adresses de diffusion sont identiques. Les informations de coût et d'ID peuvent être initialisées par le constructeur. Dans ce cas, l'administrateur ne maîtrise ni le pont racine ni la topologie. Un pont racine mal déterminé peut constituer un véritable goulet d'étranglement. En effet, chaque pont retransmet le trafic vers le port racine ainsi de suite jusqu'à ce qu'il atteigne sa destination. Si le destinataire n'est pas localisé dans la branche montante, le pont racine reçoit tout le trafic.

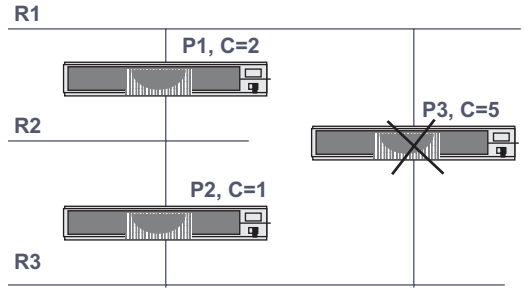


Figure 14.20 Topologie du réseaux et *spanning tree*.

Le *spanning tree* définit des routes statiques, elles ne prennent pas en compte le trafic réel sur les branches du réseau. Si on considère le réseau représenté figure 14.20. Compte tenu des coûts indiqués (C), le pont P3 est en sommeil. Si le trafic entre le segment R1 et R2 est important, le délai de retransmission des trames du segment R1 vers le segment R3 peut être important. Il eut été plus intéressant de configurer le réseau pour que le pont backup soit le pont P2, sauf si le trafic P1,P2 est important ! Le routage par la source (**SR**, *Source Routing*), étudié ci-dessous, autre mode d'acheminement dans les réseaux pontés, remédie à cet inconvénient, il détermine la route optimale dans le réseau en fonction de critères prédéfinis (charge, délai...).

14.3.5 Ponts à routage par la source

Généralités

D'origine IBM, le routage par la source (**SR**, *Source Routing*) est un mode de fonctionnement spécifique des ponts dans l'environnement Token Ring. Dans le SR, les ponts n'entretiennent aucune table d'acheminement. Ils se contentent de router les trames selon les indications

contenues dans le champ d'informations de routage (**RI**, *Routing Information*) de la trame Token Ring. Le *spanning tree* et le *source routing* ne sont pas incompatibles, la plupart des ponts dans l'environnement Token Ring utilisent les deux algorithmes.

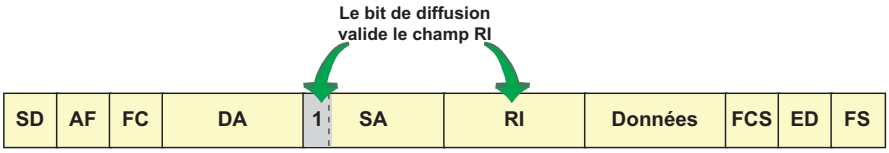


Figure 14.21 Trame MAC 802.5 validant le champ RI.

La présence d'un champ RI est indiquée par le bit multicast du champ adresse source de la trame MAC (à 0, pas de champ RI, à 1 présence du champ RI). Il contient la liste des ponts à traverser pour joindre le destinataire. La trame MAC 802.5, modifiée, est représentée figure 14.21. Dans le *source routing*, ce sont les stations et non les ponts qui entretiennent les tables d'acheminement. Ces tables peuvent être statiques (initialisées par l'administrateur) ou dynamiques (construites par la station).

Principe

Lorsqu'une station désire envoyer un message, elle consulte sa table d'acheminement (association d'une adresse MAC et d'une route à suivre). Si l'adresse MAC destination n'y est pas enregistrée, elle diffuse sur le réseau une trame de découverte.

Chaque pont, qui reçoit une trame de découverte, rediffuse celle-ci sur tous ses ports, sauf le port d'arrivée. Il y enregistre son identifiant (*Route Designator*) et, si son MTU est plus petit que le MTU enregistré, met à jour ce champ. Le destinataire reçoit ainsi de nombreuses trames de découverte (fonctionnement dit **ARE**, *All Route Explorer*). Il ne renvoie à la source que la première arrivée (meilleur chemin) en inversant le bit sens. Le fonctionnement du *Source Routing* est illustré figure 14.22.

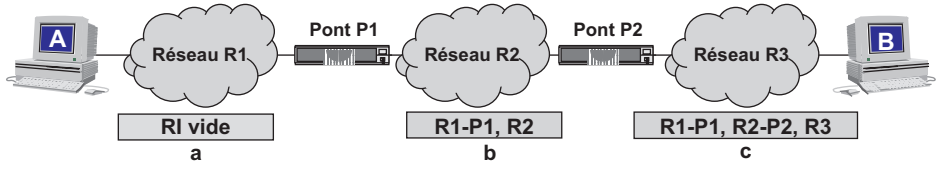


Figure 14.22 Enregistrement de route.

La station A, ignorant le chemin pour joindre B, diffuse une trame de découverte avec le champ RI vide (trame « a » de la figure 14.23). Le pont P1, à réception de cette trame, la renseigne de l'identifiant du réseau dont est issue la trame (R1), de sa propre identification (P1) et de celle du réseau sur lequel il retransmet la trame (R2), la trame contient alors les informations représentées par la trame « b ». Notons qu'il spécifie le MTU du réseau 2 et recalcule le FCS. Le pont P2 reçoit cette trame, le champ RI étant renseigné, il examine si son identifiant figure dans le champ de routage, auquel cas il détruit la trame (il l'a déjà vue). Dans le cas contraire, il renseigne la trame de son identifiant (P2) et de celui du réseau de réémission (R3). Si la valeur du champ MTU est supérieure à celle qu'il admet, il met à jour le champ MTU. La nouvelle trame est représentée en « c ». La station « B » reçoit la trame, elle apprend

© Dunod – La photocopie non autorisée est un délit

ainsi le chemin pour joindre « A » (bit sens) et accuse réception de celle-ci. À la réception de l'accusé, « A » connaît le chemin pour joindre « B ».

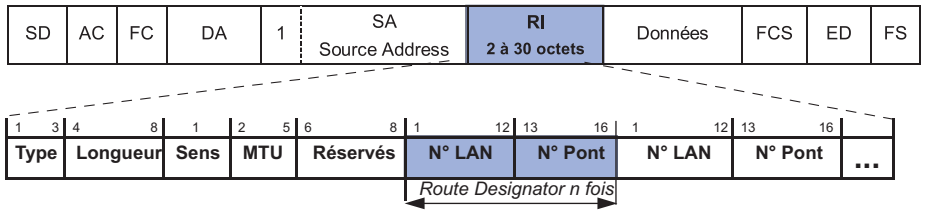


Figure 14.23 Structure du champ RI.

Le champ RI (figure 14.23), d'un maximum de 30 octets, contient les informations de :

- *type de trame*, sur 3 bits ce champ identifie la nature de la trame, vis-à-vis du source routing,
  - 001, trame d'information à router selon les informations contenues dans le champ RI,
  - 010, trame d'apprentissage **ARE** (*All Route Explorer*), cette trame est diffusée par une station qui désire connaître le chemin pour joindre une autre station et par tout pont qui la reçoit (multiple trames sur le réseau),
  - 100, trame d'apprentissage **STE** (*Spanning Tree Explorer*), mode de découverte qui réduit le trafic engendré par le fonctionnement ARE. La trame de découverte n'emprunte que les branches établies précédemment par le *Spanning Tree Protocol* ;
- *longueur*, ce champ, de 5 bits, spécifie la longueur du champ RI (de 2 à 30 octets maximum) ;
- *sens*, ce bit (S) indique si la route à suivre doit être lue de gauche à droite (S = 0, la route à suivre suit l'ordre des indications du champ RI) ou de droite à gauche (S = 1, la route à suivre suit l'ordre inverse des LAN du champ RI) ;
- **MTU** (*Maximum Transfert Unit*), ce champ de 6 bits indique la taille maximale des unités de données qui peuvent être transférées sur le réseau traversé, les valeurs sont codifiées (516, 1500, 2052, 4472, 8144, 11407, 17820, 65535) ;
- le champ **NCFI** (*Non Canonical Format Indentifier*), ce bit introduit par la recommandation IEEE 802.1Q. Il indique le format d'écriture des adresses MAC dans la trame (0 format non canonique, 1 format canonique),
- enfin, le champ route qui contient *n* sous-champs *Route Designator*. Ce champ identifie, sur 12 bits, le réseau (LAN ID) et sur 4 bits le pont traversé, à la fois en réception et en émission. Les identificateurs sont initialisés par l'administrateur de réseau.

*Les ponts SRT (*Source RoutingTransparent*)*

Pour les environnements hétérogènes, l'IEEE a spécifié (IEEE 802.1) un pont pouvant fonctionner à la fois comme pont transparent et comme pont à routage par la source.

Lorsqu'une trame est reçue par un pont, celui-ci examine le bit de multicast du champ adresse MAC source. Si ce bit est positionné, la trame est diffusée selon les informations d'acheminement du champ RI, sinon elle est émise selon l'arbre défini par le *Spanning Tree Protocol*.

Ces ponts permettent de réaliser des interconnexions dans des environnements imparfaitement connus sans se soucier d'éventuels bouclages.

14.3.6 Le pontage par translation

Le pontage par translation permet de réaliser des opérations de pontage entre réseaux différents. En principe, l'architecture d'un pont IEEE 802.3/Token Ring ou 802.3/FDDI ou encore FDDI/Token Ring (figure 14.24) ne devrait pas poser de problème, le niveau d'hétérogénéité étant le niveau MAC, le pont remonte jusqu'au niveau « trame LLC » (pont LLC).

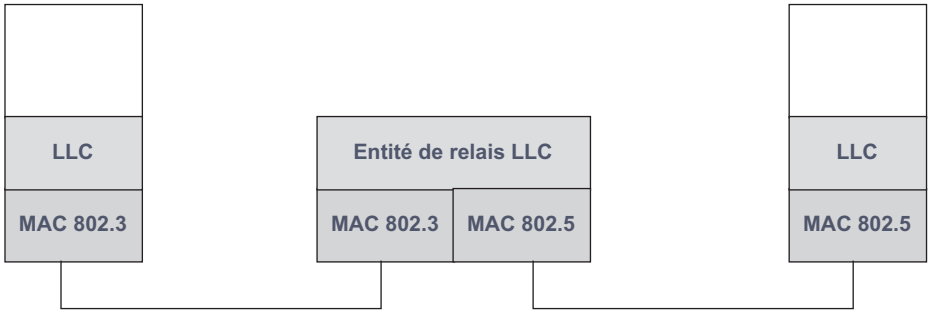


Figure 14.24 Principe de l'architecture d'un pont à translation.

Cette approche est toute théorique, en effet, les réseaux du type Ethernet n'utilisent pas l'encapsulation LLC, le pont devra alors générer le format LLC et éventuellement SNAP. Mais, la véritable difficulté réside dans la différence de taille de trame de chacun des deux réseaux. Ethernet a une taille de trame limitée à 1 500 octets. De ce fait, lorsqu'une trame Token Ring ou FDDI est de taille supérieure, celle-ci est soit abandonnée, soit fragmentée. Dans le premier cas le pont n'est pas fiable, dans le second il ne peut plus être considéré comme un pont, puisque la fragmentation n'est introduite qu'au niveau 3 du modèle de référence (modèle OSI). En pratique, les deux solutions existent.

Compte tenu de la complexité de tels ponts, il est préférable, pour réaliser l'interconnexion de réseaux différents, d'utiliser un routeur.

14.4 LES ROUTEURS

14.4.1 Généralités

Définition

Un routeur est un élément d'interconnexion de niveau 3 qui achemine (route) les données vers un destinataire connu par son adresse de niveau 3 (X.121, IP du DoD ou autre). Agissant au niveau 3 (figure 14.25), les routeurs offrent plus de possibilités que les ponts puisqu'ils

© Dunod – La photocopie non autorisée est un délit

peuvent mettre en œuvre les mécanismes du niveau 3 (segmentation, réassemblage, contrôle de congestion...).

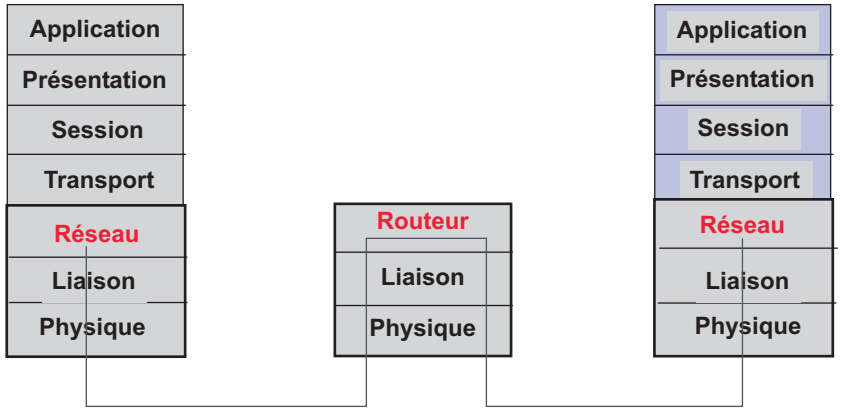


Figure 14.25 Situation des routeurs dans le modèle de l'ISO.

Routeurs et passerelles interréseau

Un routeur permet le relayage de paquets entre deux réseaux d'espace d'adressage homogène (IP/IP, ISO/ISO...). Lorsque l'espace d'adressage n'est pas homogène, par exemple interconnexion de réseaux IP via un réseau X.25, il est nécessaire de mettre en œuvre un mécanisme de conversion d'adresses (IP/ISO) non défini au niveau 3 de l'ISO. Ce dernier n'est pas défini, chaque constructeur apporte sa solution. L'organe d'interconnexion n'est plus strictement un routeur, c'est une passerelle[4] interréseau. Le langage courant continue de le désigner comme routeur.

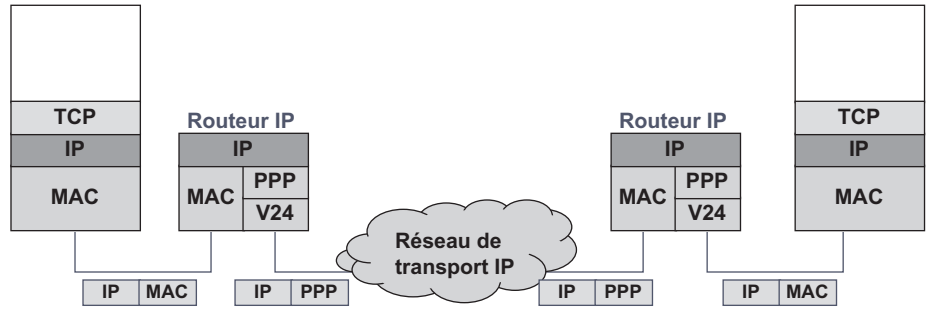


Figure 14.26 Interconnexion de réseaux homogènes.

La figure 14.26 illustre l'interconnexion de deux réseaux homogènes, ceux-ci mettent en œuvre le protocole TCP/IP et le réseau d'interconnexion utilise le protocole IP, l'espace d'adressage est identique. Les données issues d'un réseau sont encapsulées dans un protocole de liaison comme **PPP** (*Point-to-Point Protocol*).

4. Pendant longtemps, les RFC ont ignoré le terme de routeur et n'ont utilisé que celui de passerelle (*gateway*).

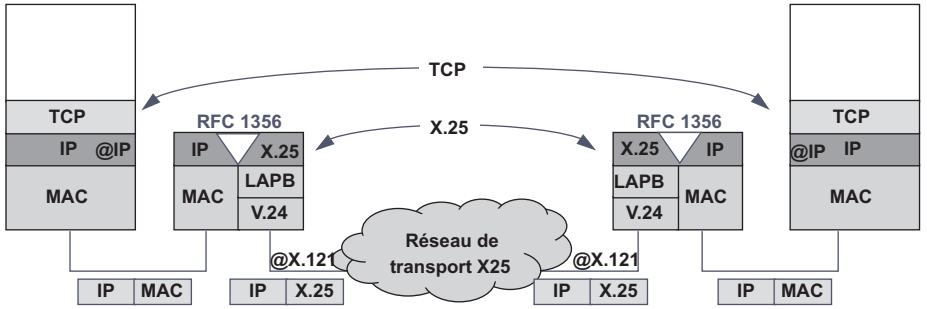


Figure 14.27 Interconnexion de réseaux hétérogènes.

La figure 14.27 illustre l'utilisation d'une passerelle interréseau. Les deux réseaux locaux IP LAN 1 et LAN 2 sont reliés via un réseau X.25 (RFC 1356). Le protocole interréseau utilisé (X.25) est totalement incompatible avec le protocole des réseaux d'extrémité (TCP/IP). Non seulement les adresses sont incompatibles (X.121 pour X.25 et IP pour TCP/IP), mais les réseaux utilisent des techniques différentes (mode datagramme pour TCP/IP et mode orienté connexion pour X.25). La passerelle devra assurer la conversion d'adresse, l'ouverture et la fermeture des circuits virtuels () pour chaque adresse IP distante.

Architecture d'un routeur

Un routeur met en relation un couple de ports d'accès (LAN ou WAN) identifiés par une adresse. Le schéma de la figure 14.28 représente l'architecture simplifiée d'un routeur.

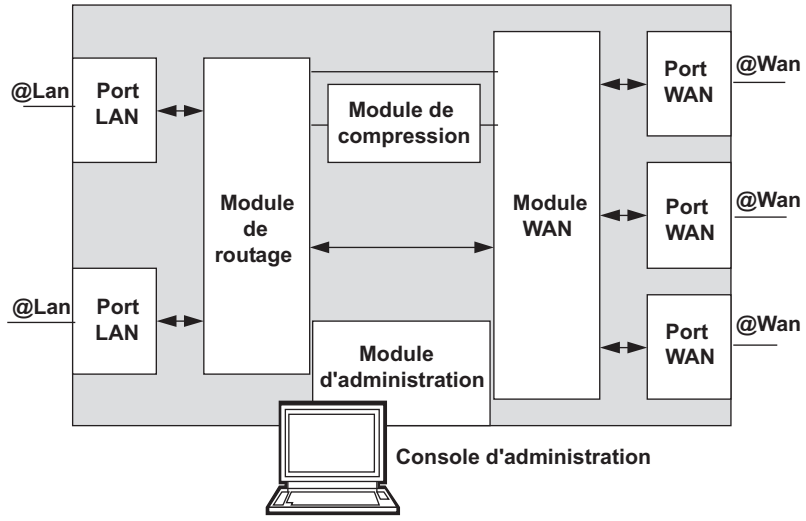


Figure 14.28 Architecture simplifiée d'un routeur.

La configuration générale d'un routeur consiste en une succession de déclarations pour effectuer la mise en relation des différents modules, et en un ensemble de paramètres décrivant leurs caractéristiques (protocole utilisé, MTU, taille fenêtre...). Un routeur n'est pas obligatoi-

© Dunod – La photocopie non autorisée est un délit

rement une machine spécifique, une station d'un réseau local peut participer à l'acheminement des données (UNIX, LINUX, Windows NT...).

14.4.2 Les techniques de routage

Généralités

Ces techniques ont été étudiées au chapitre 8. Rappelons-en le principe, les routeurs orientent les paquets selon des informations contenues dans des tables dites tables de routage. Ils utilisent essentiellement deux modes de routage :

– le routage statique ou fixe, dans ce type de routage, les tables de routage sont introduites par l'administrateur de réseau à l'initialisation du réseau ;

– le routage par le chemin le plus court, dans ce type de routage, les tables de routages indiquent pour chaque destination le coût le moins élevé. Périodiquement, des échanges d'informations entre les routeurs permettent de maintenir ces tables à jour. Les algorithmes de vecteur distance (*Distance Vector Routing*) et à état des liaisons (*Link State Routing*) sont de cette nature.

La station qui a des données à transmettre connaît le routeur auquel elle est rattachée (routeur ou passerelle par défaut). Ce routeur doit ensuite déterminer le prochain nœud à atteindre pour trouver le destinataire. Ce choix est effectué par consultation d'une table de routage en fonction d'une politique de routage. Rappelons qu'un protocole de routage n'indique pas comment est prise la décision de routage (politique de routage), il détermine seulement comment sont échangées les informations de routage. Dans la pratique ces notions sont confondues. Un protocole de routage résout essentiellement trois problèmes :

– il découvre les autres routeurs du réseau ;

– il construit les tables de routage ;

– il maintient les tables de routage à jour.

Si on veut réaliser l'interconnexion de réseaux d'opérateurs différents, il est nécessaire de définir un protocole commun d'échange des informations de routage. Chaque opérateur peut alors utiliser le mode de routage qui lui convient. Aussi, outre l'aspect de limitation du trafic de gestion, le domaine global de routage (**Internet**) a été subdivisé en domaines de routage autonomes (**AS**, *Autonomous System*). Cette division conduit à distinguer deux familles de protocoles de routage (figure 14.29) :

– les protocoles de routage intradomaine, pour le routage à l'intérieur d'un même domaine (**IGP**, *Interior Gateway Protocol*). Les paquets de service du protocole de routage identifient le domaine d'appartenance, tout paquet qui n'appartient pas au même domaine est ignoré. Cette technique limite la diffusion à l'intraréseau ;

– les protocoles de routage interdomaine (**EGP**, *Exterior Gateway Protocol*). Ces protocoles routent les paquets d'informations dans l'interréseau. Ces protocoles doivent prendre en compte les accords commerciaux ou politiques entre les systèmes autonomes. Notons que les machines d'accès à l'interréseau mettent en œuvre les deux types de protocoles, un protocole intradomaine sur leur lien intradomaine, et un protocole interdomaine sur le lien interréseaux.

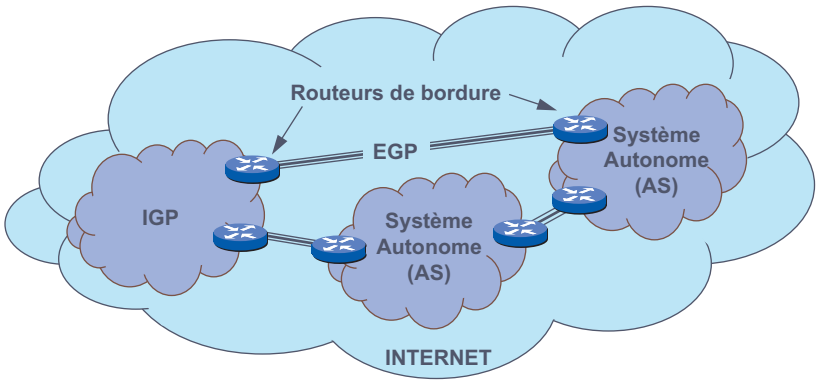


Figure 14.29 Découpage d'Internet en domaines de routage.

Le routage vecteur-distance, RIP

➤ RIP v1

Issu des travaux de Bellman-Ford, le protocole **RIP** (*Routing Information Protocol*, RFC 1058), développé par l'Université de Californie (UCB, *University of California at Berkeley*) pour UNIX BSD 4.2 (*Berkeley Software Distribution*) et utilisé initialement dans Arpanet, est en raison de sa simplicité, de sa solidité, de sa facilité de mise en œuvre et, ceci malgré ses lacunes, le protocole de routage vecteur distance le plus diffusé.

RIP distingue deux types d'équipement les actifs et les passifs. Les premiers diffusent périodiquement leur route vers les autres nœuds tandis que les seconds écoutent et mettent simplement leur table à jour en fonction des informations reçues. Un routeur fonctionnant en mode actif envoie toutes les 30 secondes un message de diffusion[5] pour signaler qu'il connaît une route pour accéder à un réseau et en signale le coût en nombre de sauts.

RIP v1 présente plusieurs inconvénients. Il ne contient aucune information sur le masque de sous-réseau, par conséquent le routeur doit, d'une part, disposer localement de cette information et d'autre part le masque de sous-réseau doit être identique sur tout le réseau. Il ne supporte pas le trafic multicast.

Dans les grands réseaux, la diffusion des tables toutes les 30 s induit un trafic important et un temps de convergence (stabilisation des tables) conséquent qui peut être de plusieurs minutes. Pour limiter ce temps, la visibilité d'un routeur n'est que de 15 sauts, une métrique de 16 représente une route non joignable. Il n'y a pas d'accusé de réception des messages. Si on ne reçoit aucun message durant 180 s, la route silencieuse est déclarée inaccessible. Lorsqu'un routeur est arrêté par la procédure normale d'extinction, il envoie, à ses voisins, sa table avec tous les liens à 16. Cette procédure permet une convergence plus rapide vers la nouvelle situation. D'autres solutions sont mises en œuvre pour améliorer la convergence et éviter les boucles :

– *Split horizon* ou horizon coupé, les données de routage ne sont pas renvoyées vers le nœud d'où on les a apprises ;

5. Le principe de fonctionnement du routage vecteur distance a été expliqué section 8.5.2.

© Dunod – La photocopie non autorisée est un délit

– *Poison reverse*, complète le *split horizon*. Si, après avoir détecté une route coupée, un routeur reçoit une information d'accessibilité avec un coût important par rapport au coût initial il ignore cette information. Il estime alors que le message lui est revenu par une boucle,

Lorsqu'une nouvelle route est annoncée, si le routeur contient déjà une entrée de même coût dans sa table, il ignore cette information. De ce fait, non seulement RIP ne peut faire d'équilibrage de charge mais, dans un réseau maillé, le chemin est dépendant de l'ordre de mise en marche des routeurs.

Les messages ne sont pas authentifiés. Il est alors possible à un individu malveillant de générer des messages RIP avec des coûts tels que toutes les routes passent par un même routeur. Le nœud ainsi attaqué devient alors un véritable goulet d'étranglement, le réseau peut ainsi être complètement paralysé (congestion).

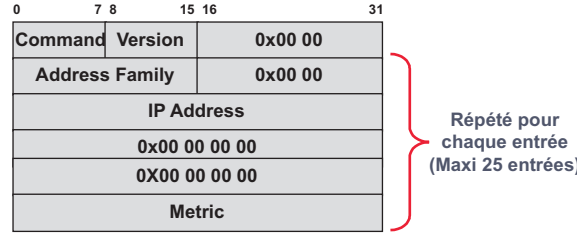


Figure 14.30 Message RIP v1.

La taille maximale d'un message RIP (figure 14.30) est de 512 octets de charge utile, auxquels il convient d'ajouter 28 octets pour l'en-tête UDP (port 520) et IP. Cette taille limite le nombre d'entrées dans un message à 25. Le message comporte les informations suivantes :

– le champ *command* permet de distinguer les différents types de message
  – 1, *Request*, permet de demander à un système distant d'envoyer tout ou partie de sa table de routage. Ce message permet, à un routeur, lors de son démarrage d'acquérir rapidement les informations de routage sans attendre une diffusion ;
  – 2, *Response*, message contenant tout ou partie d'une table de routage. Ce message peut être envoyé en réponse au message précédent (*Request*), ou lors d'une simple mise à jour périodique ;
  – 3 et 4 *traceon* et *traceoff*, ces messages aujourd'hui obsolètes, doivent être ignorés ;
  – 5, réservé à Sun Microsystems ;
  – 6, réservé à d'éventuelles nouvelles commandes ;
– le champ *Version* identifie la version du protocole, il doit être mis à 1 ;
– l'ensemble des champs suivants contient les informations en relation avec les routes :
  – *Address Family* identifie la famille d'adresse, cette valeur est à 2 pour IP. Toute autre valeur doit être ignorée. Les deux octets suivants doivent être mis à zéro ;
  – *IP Address* contient l'adresse IP d'un réseau, d'un sous-réseau ou d'une station ou un routeur par défaut (0.0.0.0) ;
  – les deux champs suivants doivent être mis à zéro ;

– *Metric* indique en nombre de sauts la distance du réseau IP identifié précédemment. La valeur maximale est de 15.

Le protocole **IGRP** (*Interior Gateway Routing Protocol*) de Cisco remédie à de nombreux inconvénients. Dans RIP, la variable étant le nombre de sauts, une voie plus rapide (débit) est ignorée si le nombre de sauts est plus important. IGRP utilise une métrique, configurable par l'administrateur, qui permet de privilégier un lien :

$$M = F \times \left(\frac{k_1}{D \times (1 - C)} + \frac{k_2}{T} \right)$$

avec M : valeur de la métrique, F : coefficient indiquant la fiabilité de ligne (la valeur 255 indique un taux de perte de 100 %), D : débit du lien, C : charge du lien, T : somme des temps de traitement, d'émission et de propagation d'un datagramme. Les coefficients k_1 et k_2 sont des facteurs de pondération fixés par l'administrateur, ils peuvent être modifiés dynamiquement en fonction de la valeur du champ TOS (*Type Of Service*).

IGRP permet en outre, la prise en compte des masques de sous-réseaux, le partage de charge et la limitation des domaines de diffusion en introduisant la notion de systèmes autonomes.

➤ RIP V2 (RFC 1721 à 1724)

Mettant à profit les champs non utilisés de RIP v1, RIP v2 remédie à certains inconvénients de RIP v1 tout en restant compatible avec lui. RIP v2 permet de diffuser le masque de sous-réseau (*Subnet Mask Field*). Le masque envoyé est appliqué à l'adresse IP en cours d'envoi. Un champ d'authentification peut être inséré entre l'en-tête RIP et la première entrée. Ce champ est repéré par la valeur « *address family ID* » à 0xFFFF. La figure 14.31 compare le format du message RIP v1 et RIP v2 avec authentification simple.

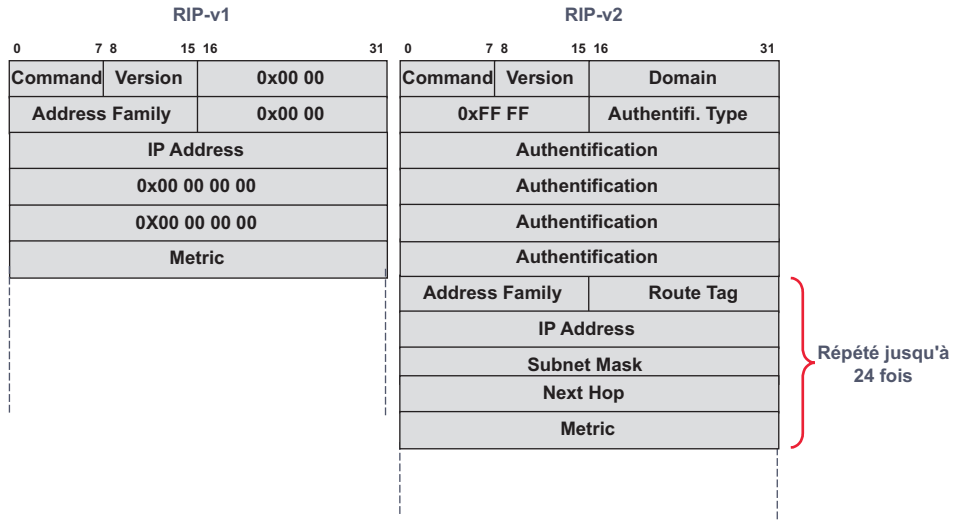


Figure 14.31 Format des messages RIP v2.

Le champ *Type authentification* à 0x0000 indique qu'il s'agit d'une authentification simple, suit le mot de passe en clair sur 16 octets. Un autre format, plus complexe, permettant de crypter le mot de passe a été défini.

© Dunod – La photocopie non autorisée est un délit

Le champ *Domain* permet de subdiviser le réseau en différents réseaux logiques. Les routeurs ignorent les messages émanant d'un domaine autre que le leur. Le *champ Address Family* a la même signification. Cependant, le nouveau champ *Route Tag* pourra être utilisé en conjonction avec un protocole de routage externe (EGP). Le champ *Next Hop* identifie le routeur d'origine, mais il permet aussi de forcer une route vers un autre routeur.

RIP v2 peut fonctionner en mode broadcast et en mode multicast. L'utilisation du mode multicast permet dans un environnement mixte aux RIP v1 d'ignorer les messages adressés à l'adresse multicast 224.0.0.9.

Si RIP v2 pallie de nombreuses insuffisances de RIP v1, sa portée, toujours limitée à 15 sauts, le destine aux petits et moyens réseaux.

Le routage à état des liens (OSPF)

➤ Généralités

Contrairement au protocole à vecteur distance, le protocole à état des liens ne diffuse, sur le réseau, que les modifications qu'il a détectées dans la topologie du réseau, lien inaccessible, coût modifié... Chaque nœud entretien une base de données qui est le reflet total de la cartographie du réseau. Cette vision globale, par chaque routeur, du réseau permet d'éviter la formation de boucle. Le coût de la liaison (métrique) est configurable interface par interface, plusieurs métriques peuvent être utilisées simultanément (longueur de la file d'attente, débit, distance...). À partir de ces éléments, chaque routeur calcule la route de moindre coût selon l'algorithme de Dijkstra[6].

OSPF (*Open Shortest Path First*) est capable d'assurer un routage par type de service (champ TOS du datagramme IP), il peut aussi assurer l'équilibrage de charge entre plusieurs routes de même coût.

Lorsque le réseau est important, la diffusion des messages et la détermination de la nouvelle table de routage pénalise les performances globales du réseau. Aussi, OSPF a introduit la notion d'aires limitant ainsi l'espace de diffusion et le volume de calcul à effectuer.

➤ Notion d'aires de routage

Une aire ou zone (*area*) correspond à une subdivision logique d'un réseau OSPF (figure 14.32). Il est important de ne pas confondre la notion d'aire d'OSPF et celle de système autonome (**AS**, *Autonomus System*). Un AS est constitué d'un ou plusieurs réseaux sous la responsabilité administrative d'une même autorité. Les protocoles de routage utilisés dans chacun des AS peuvent être différents, un protocole spécifique (**EGP**, *External Gateway Protocol*) gère l'échange d'information entre les différents AS. Tandis que les différentes aires OSPF utilisent toutes le protocole OSPF.

La hiérarchie introduite par OSPF est limitée à 2 niveaux. L'environnement OSPF comprend les éléments suivants :

– une zone dite fédératrice (*area backbone*) assure l'interconnexion de toutes les autres zones. Chaque zone est identifiée par un numéro de zone unique sur 32 bits, ce numéro est un identifiant et non une adresse IP. Le numéro 0.0.0.0 identifie la zone fédératrice. Le backbone

6. Le principe de fonctionnement du routage à état des liens a été expliqué section 8.5.2.

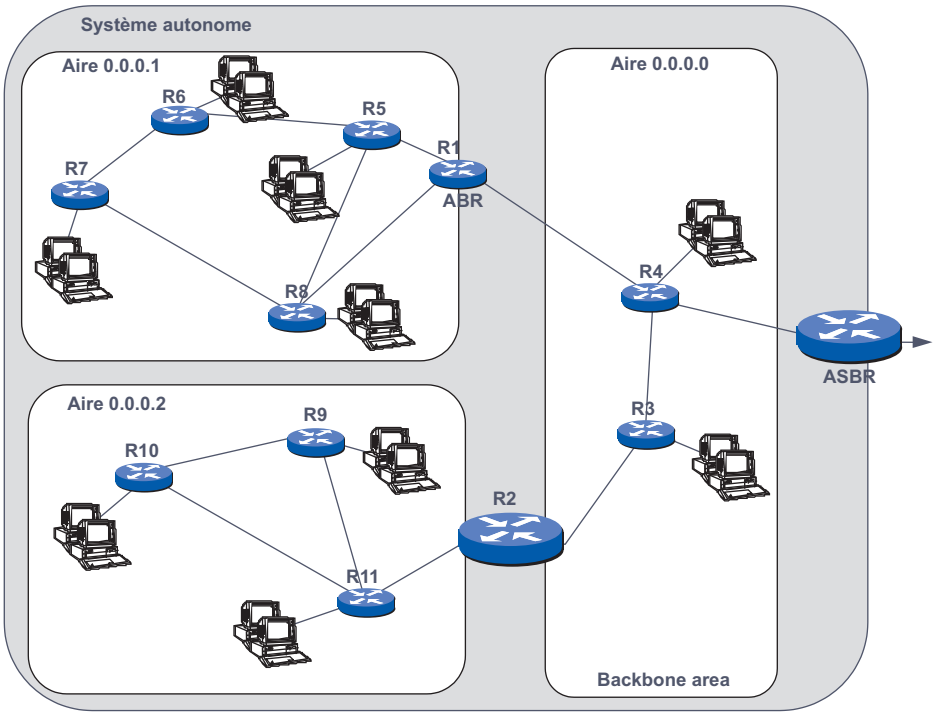


Figure 14.32 Les aires OSPF.

assure l'acheminement interzone. Si le réseau OSPF ne comporte qu'une seule zone, cette zone est obligatoirement la zone 0.0.0.0 ;

– des routeurs de zone ou *Internal Router* (**IR**), ces routeurs n'annoncent que les routes internes à leur zone. En principe, on limite une zone à 50 routeurs au maximum ;

– des routeurs qui assurent la connexion au backbone, et qui annoncent les routes extérieures à la zone. Sur la figure 14.32, il s'agit du routeur R1 (**ABR**, *Area Boundary Router*), le routeur R2 qui correspond à une interface locale entre la zone 2 et la zone 0 est considérée comme appartenant au backbone ;

– des routeurs frontières de système autonome (**ASBR**, *Autonomous System Boundary Router*). Ces routeurs assurent l'échange d'information avec les autres systèmes autonomes. Les routes extérieures au système autonome sont apprises par des protocoles autres qu'OSPF (routage statique, EGP, BGP...)

La réduction du nombre de routeurs par zone de diffusion limite le trafic de gestion mais les échanges entre routeurs sont encore nombreux. Ils varient comme le carré du nombre de nœuds. En effet, si N est le nombre de routeurs, le nombre de liens est $N\ (N-1)/2$, le nombre d'annonces est donc de $N\ (N-1)$. Pour limiter ce trafic OSPF introduit, la notion de routeur désigné (**DR**, *Designated Router*). C'est ce dernier qui assurera la diffusion des messages vers les routeurs de la zone ce qui ne nécessite que N messages (1 message vers le DR et $N-1$ message du DR vers les hôtes). L'élection du routeur désigné est similaire à celle du moniteur du réseau Token Ring. Dans les réseaux **NBMA** (*Non Broadcast Multiple Access*), il faut configurer chaque routeur avec la liste des adresses des routeurs de l'aire et de leur priorité.

© Dunod – La photocopie non autorisée est un délit

L'administrateur réseau affecte une priorité (0 à 255) à chaque routeur. Un routeur de priorité 0 ne pourra jamais être élu routeur désigné. Pour une zone donnée, c'est le routeur de plus haute priorité qui est désigné. En cas d'égalité c'est le routeur de plus grand identificateur qui est élu. L'identificateur est en principe l'adresse IP qui désigne le routeur. Un routeur désigné de *backup* est aussi élu. Lorsqu'un routeur est mis sous tension, il écoute le trafic et apprend ainsi quel est le routeur désigné et son *backup*. Il accepte ces informations, même si sa priorité est plus grande. C'est l'absence de trafic en provenance du routeur désigné qui permet de détecter sa panne et de déclencher le mécanisme d'élection.

➤ L'agrégation de routes

L'utilisation de zones offre un mécanisme puissant d'affectation des adresses IP. Si tous les réseaux ou sous-réseaux d'une zone ont des adresses IP contiguës, le routeur ne signale qu'une seule route aux autres routeurs. Cette propriété permet d'une part de minimiser le trafic d'annonce et, d'autre part, d'alléger les tables de routage La figure 14.33 illustre ce principe.

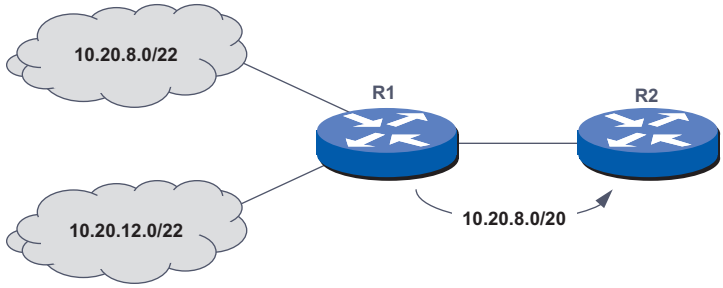


Figure 14.33 L'agrégation de routes dans OSPF.

En routage vecteur distance, les deux sous-réseaux de la figure 14.33 seraient annoncés individuellement et constitueraient 2 entrées dans les tables de routage de R1 et de R2. En OSPF, le routeur R1 considère que les réseaux ont en commun les 20 premiers bits, il n'annonce que cette seule information. Pour éviter d'éventuels conflits, les tables de routage classent en premier les plus grands préfixes.

➤ Fonctionnement succinct d'OSPF

Directement au-dessus d'IP (protocole 87), OSPF, sur les réseaux à diffusion, utilise des adresses multicast, 224.0.0.5 pour adresser tous les routeurs de l'aire et 224.0.0.6 pour communiquer avec le routeur désigné. Tous les messages d'OSPF utilisent le même en-tête de 24 octets (figure 14.34).

Les différents champs sont :

- Version, sur 1 octet, indique la version courante du protocole. La version actuelle est la 2 ;
- Type, sur un octet précise le contenu du champ données :
  - Type 1, message *Hello* pour déterminer le délai ;
  - Type 2, message de description de la base de données (topologie) ;
  - Type 3, requête d'état de la liaison (*Link State Request*) ;
  - Type 4, message de mise à jour de l'état de la liaison (*Link State Update*) ;

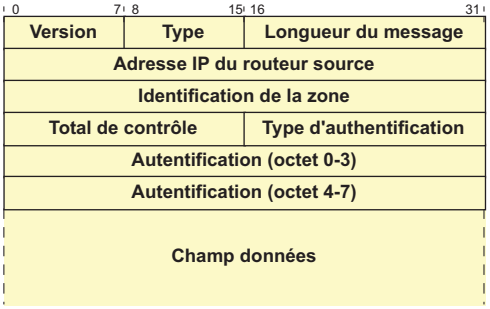


Figure 14.34 En-tête des messages OSPF.

  - Type 5, acquittement d'un message d'état de la liaison ;
- Le champ longueur du message indique en octets la longueur du message en-tête compris ;
- Adresse IP de l'expéditeur du message ;
- Identification de zone, numéro d'identification sur 32 bits de la zone (*area*). Un routeur peut être multidomicilié (*multi-homed*), c'est-à-dire qu'il peut avoir une interface sur plusieurs aires. Cette information est donc complémentaire de celle de l'hôte ;
- Total de contrôle, calculé de manière similaire au total de contrôle IP ;
- Type d'authentification, 0 aucune, 1 mot de passe simple ;
- Authentification contient un mot de passe en clair sur 8 caractères.

Le fonctionnement d'OSPF peut se décomposer en quatre étapes :

- élection du routeur désigné et de son backup ;
- synchronisation des données topologiques ;
- mise à jour des bases de données ;
- calcul du chemin le plus court.

Pour son fonctionnement OSPF met en œuvre trois sous-protocoles :

- le protocole Hello utilisé entre deux routeurs adjacents pour synchroniser leur base de connaissance ;
- le protocole d'échange permet, lors de l'initialisation d'un routeur, l'acquisition des entrées de sa base de données ;
- le protocole d'inondation est utilisé par un routeur pour signaler la modification de l'état d'un lien qui lui est rattaché.

Le protocole Hello

Le protocole Hello[7] permet de vérifier la connectivité entre les nœuds, d'élire le routeur désigné et le routeur backup. Un message *Hello* (figure 14.35) est envoyé périodiquement (intervalle *Hello*) pour tester la présence du routeur voisin. En l'absence de réception de message

7. Attention, il ne faut pas confondre le sous-protocole Hello d'OSPF avec l'ancien protocole de routage Hello, aujourd'hui obsolète.

© Dunod – La photocopie non autorisée est un délit

durant une période supérieure à une durée prédéterminée dénommé **intervalle de mort**, la liaison silencieuse est déclarée inaccessible.

Dans les réseaux à diffusion l'élection du routeur désigné se fait par écoute du trafic tandis que dans les réseaux NBMA, le message Hello est adressé à chaque routeur éligible (priorité non nulle). Lors de sa mise sous tension, le routeur ne connaît pas le routeur désigné, les champs routeur désigné et backup sont mis à 0 (0.0.0.0). Si un routeur désigné et son backup existent, ceux-ci sont acceptés par tout nouveau routeur même si sa priorité est plus forte.

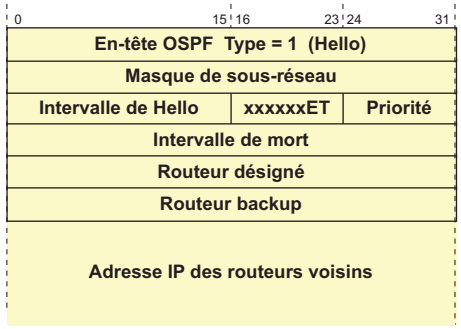


Figure 14.35 Message Hello.

Le message Hello contient la liste des routeurs identifiés par écoute ou réception de messages Hello. Lorsque la liste comprend sa propre adresse, le routeur en déduit que la connectivité avec son voisin est complète (connectivité bilatérale).

Le champ options décrit les options supportées par le routeur. Seuls deux bits sont utilisés. Le bit E à 1 indique que le routeur émet et reçoit des routes externes. Ce bit doit avoir la même valeur pour les deux routeurs d'extrémité d'une même liaison. Le bit T informe que le routeur a la possibilité de prendre en compte le champ TOS des datagrammes IP et de router en fonction de celui-ci.

Le protocole d'échange

Après découverte de ses voisins, le routeur doit initialiser sa base de données topologiques. Les différentes informations fournies lui permettront de construire les entrées de la table (liste des liens et routeurs responsables de la mise à jour des valeurs d'état ou coût). Ces entrées permettront de construire une liste de demandes d'état de liens. Par la suite, les différents champs de la base seront maintenus à jour par le protocole d'inondation.

L'échange peut avoir lieu entre routeurs adjacents ou avec le routeur désigné. Durant cette phase le routeur ayant initialisé l'échange est déclaré maître (*Master*) et l'autre esclave (*Slave*). En cas de collision d'initialisation, c'est le routeur de plus grand identifiant qui est choisi. La figure 14.36 représente le format du message (message OSPF de type 2).

Le champ MTU informe le routeur de la taille maximale des datagrammes supportée sur le lien. Le champ option est identique à celui du message *Hello*. Dans le champ suivant, le bit *I* à 1 indique qu'il s'agit du premier message de description (*Initialize*), le bit *M* (*More*) informe qu'un ou des messages suivent ; tandis que le bit *MS* (*Master/Slave*) à 1 indique que l'émetteur est le maître. Le numéro de séquence permet de contrôler l'échange, seul le maître l'incrémente de 1 à chaque message envoyé. L'esclave recopie ce numéro dans son message

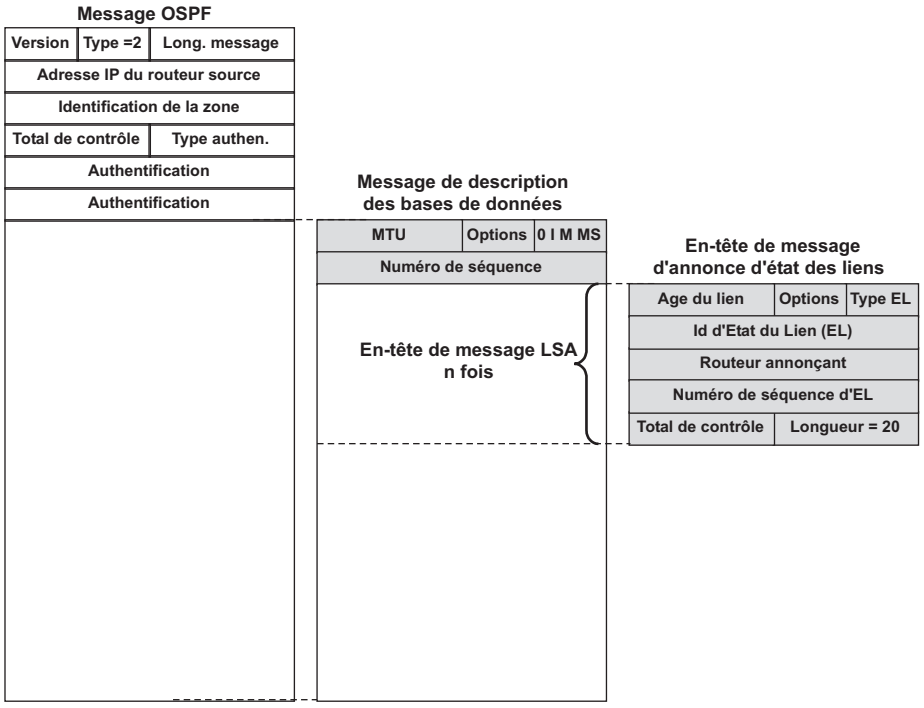


Figure 14.36 Message de description de la base de données.

d'acquittement (message de description de sa base de données avec le bit *MS* = 0, ce message pouvant éventuellement être vide).

Vient, ensuite, la description des entrées de la table des liaisons. Ce descriptif est en fait l'en-tête des messages d'annonce de l'état d'une liaison (**LSA**, *Link State Advertissement*). Chaque lien y est décrit très précisément. Le champ âge du lien indique en seconde le temps écoulé depuis la première annonce du lien. Le champ option est identique à celui du message Hello. L'information type d'état du lien (**EL**) peut prendre 5 valeurs selon la nature du routeur annonçant :

– Type 1, (*Router Link*), le routeur annonçant est un routeur interne à l'aire, le champ ID de l'état des liens indique son identifiant. Dans les messages d'état des liens, cet en-tête est suivi de la liste des liens et de leurs caractéristiques (voir figure 14.37) ;

– Type 2, *(Network Link*), le routeur est un routeur interne d'un réseau NBMA (sans diffusion), l'identifiant d'état des liens est alors l'adresse du routeur désigné. Dans les messages d'état des liens, cet en-tête est suivi de la liste des routeurs qui ont établi une relation de voisinage avec le routeur désigné ;

– Type 3, (**ABR**, *Area Boundary Router*), il s'agit alors d'un routeur de bordure d'aire, l'ID d'état des liens contient l'adresse IP du lien annoncé. Dans les messages d'état des liaisons, cet en-tête est suivi de la liste des routeurs de la zone accessibles par cette voie et le masque de sous-réseau associé ;

– Type 4, ce type de message est similaire au précédent mais s'adresse à un routeur d'aire terminale ;

© Dunod – La photocopie non autorisée est un délit

– Type 5, (**ASBR**, *Autonomous System Boudary Router*), le routeur est en bordure de système autonome. L'ID d'état des liaisons correspond à l'adresse IP de la liaison. Dans les messages d'état des liaisons, cet en-tête est suivi de la liste des liens connus et de leurs caractéristiques.

Dans les différents messages échangés, l'association de l'identifiant du routeur annonçant (celui à l'origine des informations concernant ce lien), de l'identifiant d'état des liens et du type d'état des liens distingue de manière unique un enregistrement. Le champ numéro de séquence identifie une annonce. Le total de contrôle porte sur tout le message d'annonce d'état d'un lien. Dans le message de description de la base de données le champ données étant absent, le total de contrôle ne porte que sur les 20 octets d'en-tête LSA.

Chacun des routeurs participant à l'échange construit, pour les liens dont il n'a pas le descriptif ou pour lesquels l'information est trop vieille, une liste d'état des liens à demander. La structure de ce message (OSPF type 3) est représentée figure 14.37, la signification des champs est identique à celle du message de description de la base de données.

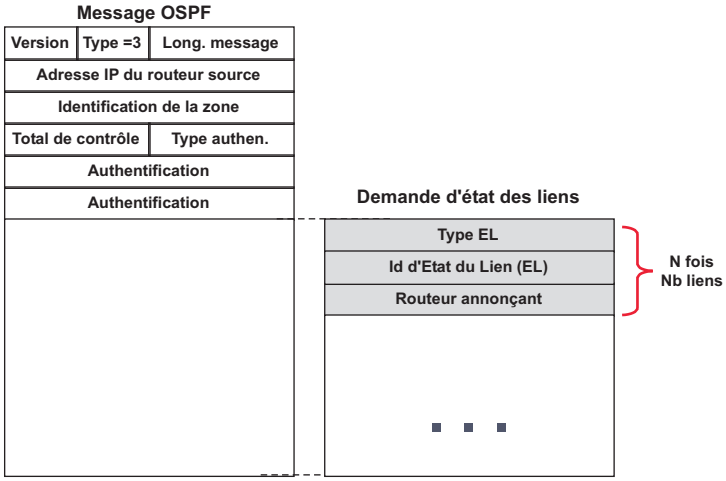


Figure 14.37 Message de demande d'état des liens.

Le routeur cible renvoie un message de mise à jour des liens (*Link State Update*) dont le contenu dépend du type d'état des liens. Les messages de mise à jour de l'état des liens des types EL = 1 décrivent les liens, les messages LSA des types EL = 2, 3, 4 donnent une liste de réseaux et les masques associés, le type EL = 5 décrivent les liens externes. La figure 14.38 donne le format d'un message de mise à jour pour un EL de type 1.

L'en-tête de description d'un lien précise la nature du routeur annonçant (bit **V** pour *Virtual*, routeur en extrémité d'un lien virtuel ; bit **E** pour *External*, routeur en frontière d'un système autonome ; **B** pour *Border*, routeur en bordure d'aire). Le champ significatif suivant indique le nombre de liens décrits pour ce routeur. Le tableau de la figure 14.39 indique en fonction de la valeur du champ *Type*, la signification du champ d'identification du lien et du champ données du lien.

Enfin, la métrique est indiquée. OSPF peut gérer plusieurs tables de routage et router en fonction du TOS. Les routeurs qui ont cette possibilité positionnent à 1 le bit T de l'en-tête du message d'état des liens (champ option). La partie descriptive du message d'état des liens fournit, pour chaque lien, une métrique par TOS géré. Le routage sera déterminé selon la valeur du champ TOS du datagramme IP (figure 14.40).

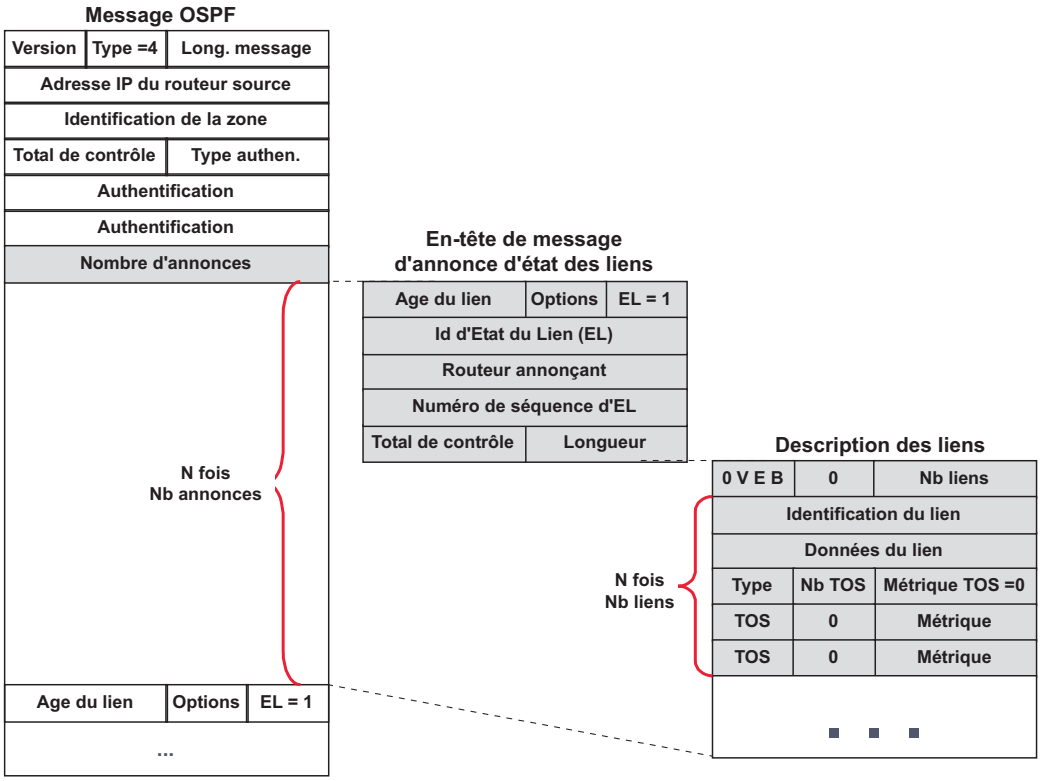


Figure 14.38 Message d'annonce d'états des liens (EL = 1).

Type	Type de lien décrit	ID du lien	Données du lien
1	Lien point à point vers un autre routeur	Identification du routeur distant (généralement son adresse IP)	Adresse IP de l'interface
2	Connexion à un réseau de transit	Adresse IP du routeur désigné	Adresse IP de l'interface
3	Connexion à un réseau terminal	Adresse du réseau IP	Masque de sous-réseau
4	Lien virtuel	Identification du routeur distant	Adresse IP d l'interface

Figure 14.39 Signification des champs Identification et Données du lien.

Codage OSPF	Valeur des bits du champ TOS				Description du service invoqué
	Délai	Débit	Fiabilité	Coût	
0	0	0	0	0	Service normal
2	0	0	0	1	Minimiser le coût financier
4	0	0	1	0	Maximiser la fiabilité
8	0	1	0	0	Maximiser le débit
16	1	0	0	0	Minimiser le délai

Figure 14.40 Service et valeur du TOS (Datagramme IP).

© Dunod – La photocopie non autorisée est un délit

Si un routeur n'a pas la possibilité de router en fonction du TOS, il ne participera au routage des datagrammes qui invoquent un service en fonction du TOS. OSPF ne précise pas la manière dont sont calculées les métriques. L'administrateur du réseau peut ainsi privilégier tel ou tel lien, voire interdire un lien. Par exemple, si on ne veut pas que les données transitent via un réseau facturé au volume, il suffit de porter la métrique de ce lien à 65 535. En principe, la métrique d'un lien en fonction du débit correspond au temps mis pour transmettre un volume de 10^8 bits (Métrique = 10^8/Débit de l'interface).

Les messages *Link Status Update* sont acquittés par message OSPF de type 5. La figure 14.41 décrit ce message. La signification des champs est identique à celle déjà fournies.

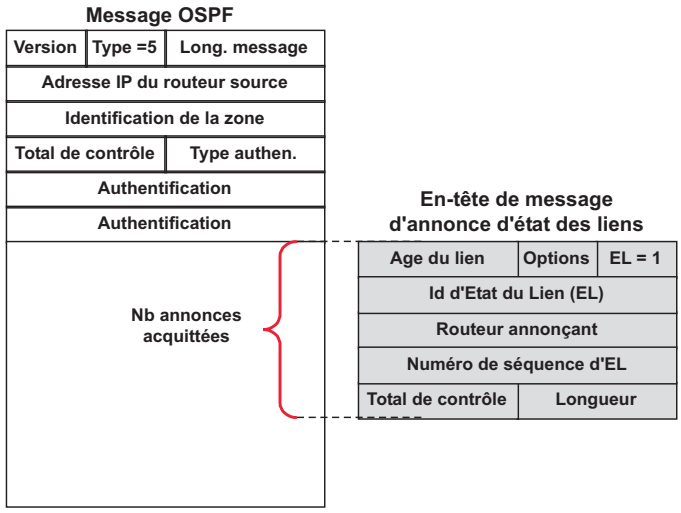


Figure 14.41 Message d'acquittement d'annonce d'état des liens.

À l'aide de ces informations, chaque routeur établit une arborescence du chemin le plus court (*Shortest Path Tree*) où il est la racine de l'arbre (algorithme de Dijkstra). Sur la base de cette arborescence, il génère sa ou ses tables de routage.

Le protocole d'inondation

À chaque changement d'état d'un lien le routeur qui en a la charge (routeur annonçant) émet un message d'avertissement d'état d'un lien (LSA, OSPF type 4, figure 14.38). Chaque routeur recevant ce message compare le numéro de séquence des liens qu'il a en mémoire et le numéro de séquence de l'annonce. Si l'annonce est plus récente, il la retransmet sur toutes ses interfaces, sauf celle par laquelle il l'a reçue et acquitte ce message (OSPF type 5, figure 14.41). Tout message reçu doit être acquitté. L'acquittement peut être implicite. Si l'annonce est faite vers le routeur désigné, celui-ci retransmet à tous les routeurs (adresse de diffusion) le message. La réception de ce message en provenance du routeur désigné vaut acquittement.

➤ Conclusion

OSPF est un protocole de routage complexe. Complexe dans sa mise en œuvre (plan d'adressage, initialisation des métriques...), complexe dans son fonctionnement (temps de calcul...). Bien qu'OSPF remédie aux principaux inconvénients de RIP (temps de convergence,

boucle...), le monde des réseaux d'entreprise est encore largement dominé par des protocoles du type vecteur distance que ceux-ci soient normalisés (RIP) ou d'origine constructeur par exemple **IGRP** (*Interior Gateway Routing Protocol*) et **EIGRP** (*Enhanced Interior Gateway Protocol*) de chez Cisco.

Le choix, pour une entreprise de tel ou tel protocole de routage est un choix stratégique. Quelles que soient les qualités des protocoles propriétaires, ils sont et demeurent propriétaires ce qui peut constituer un handicap lors de l'évolution du réseau ou du renouvellement des équipements.

Le routage interdomaine

Un système autonome (AS) correspond à un domaine de routage[8] sous le contrôle d'une autorité d'administration unique. Les différents systèmes autonomes composant l'Internet doivent s'échanger leurs informations d'accessibilité. Ainsi, chacun des routeurs de bordures des deux systèmes autonomes de la figure 14.42 doit d'une part établir une connectivité entre eux et, d'autre part informer leur voisin des réseaux qu'ils savent atteindre.

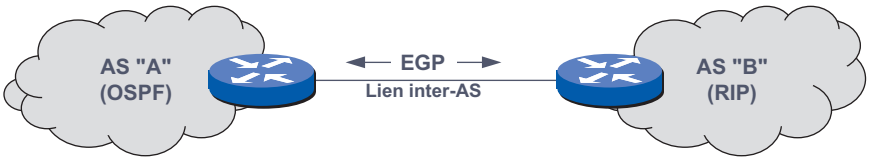


Figure 14.42 Connectivité de deux systèmes autonomes.

Ainsi, le routeur de bordure de l'AS « A » annonce au routeur de bordure de l'AS « B » par l'intermédiaire d'un protocole de routage interdomaine (**EGP**, *External Gateway Protocol*) les informations (liste d'accessibilité) qu'il a acquises, par un protocole de routage intradomaine (**IGP**, *Interior Gateway Protocol*), sur les réseaux accessibles par transit dans sa zone. Le routeur B va diffuser ces informations au format de l'IGP utilisé dans sa zone.

Le protocole de routage externe doit résoudre de nombreux problèmes spécifiques. Le premier concerne le routage politique. Supposons qu'une entreprise internationale dispose d'un réseau privé. Afin de minimiser le trafic sur son réseau, elle dispose d'un accès à Internet dans chacun des pays desservis par son réseau (figure 14.43). Cette entreprise s'oppose évidemment à ce que le trafic Internet transite par son réseau.

Le second, mis en évidence par la figure 14.42, concerne les métriques. Quelle métrique utiliser dans les annonces puisque chacun des AS peut utiliser un protocole de routage interne différent et transparent à l'EGP ? Le coût annoncé est donc forfaitaire (distance arbitraire), il permet en outre aux administrateurs de favoriser le transit par tel ou tel réseau en fonction d'accords commerciaux ou autres. Ce qui répond à la préoccupation précédente.

De nombreux protocoles de routage externes ont été testés. Actuellement Internet met en œuvre **BGP 4** (*Border Gateway Protocol*). Les informations de routage échangées comprennent : le numéro de système autonome, la liste des réseaux de chaque système autonome, la distance relative vers chacun des sous-réseaux de l'AS et l'adresse IP du routeur d'accès à ces réseaux. BGP prend en compte des critères extérieurs aux domaines de routage

8. Le concept de systèmes autonomes a été défini à la section 8.5.2.

© Dunod – La photocopie non autorisée est un délit

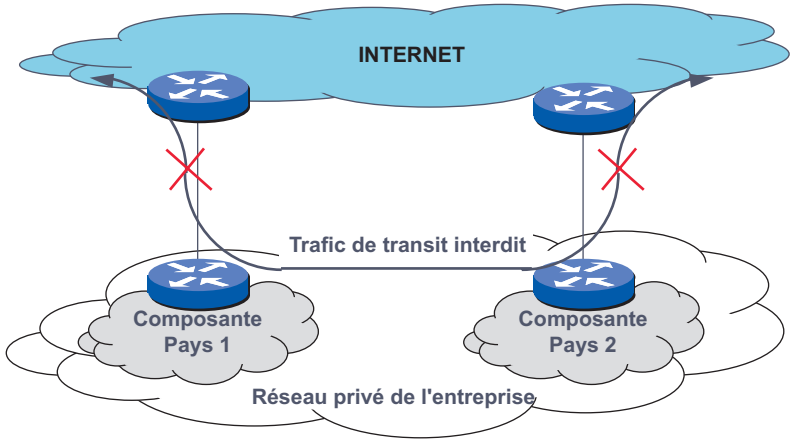


Figure 14.43 Problématique du routage politique.

(routage politique), il met en œuvre des mécanismes de détection et de suppression des boucles. BGP utilise quatre types de messages :

– les messages d'ouverture, utilisés lors de l'ouverture d'une session BGP entre deux routeurs, ils contiennent le numéro d'AS du système autonome émetteur et délai au bout duquel, si le destinataire ne reçoit aucun message, il doit considérer le routeur source comme défaillant ;

– les messages de mise à jour, utilisés pour signaler, au routeur BGP voisin (*peer router*) le changement d'état d'une ou plusieurs routes gérées par le routeur source (nouvelle route ou route devenue inaccessible) ;

– les messages de notification, utilisés pour clore une session BGP. Ils indiquent le motif de la fermeture de session ;

– les messages Hello (*Keep Alive*), ils ne contiennent aucune information, et sont utilisés par un routeur pour signaler, en l'absence de trafic, sa présence au routeur *peer*.

14.4.3 Routage et qualité de service

Généralités

La qualité de service (**QoS**, *Quality of Service*) constitue un axe de recherche majeur dans les réseaux. Deux approches ont déjà été étudiées : la réservation de ressource (réseaux à état) et la prioritisation des flux (réseaux sans état). ATM et Frame Relay appartiennent à la première catégorie, ils mettent en œuvre des mécanismes de contrôle d'admission pour garantir ainsi à chaque nouvelle connexion qu'un service minimal lui sera rendu. En ce qui concerne les réseaux IP, aucun état n'est maintenu dans le réseau (réseau datagramme ou *best effort*), dans ce contexte seule l'approche de prioritisation semble possible.

Conçu à une époque où les seuls flux applicatifs à acheminer étaient tous de même nature, IP n'implémentait qu'un mécanisme simple, aujourd'hui obsolète, de qualité de service défini selon 3 bits, D (*Delay*), T (*Troughput*) et R (*Reliability*) du champ TOS. Le champ TOS a été redéfini par la RFC 1812 (*IP Precedence*[9]). Le traitement dans le réseau de flux sensibles au

9. Voir section 10.4.2.

temps de transfert comme le trafic SNA et les applications multimédias ont montré la nécessité de définir des mécanismes spécifiques pour garantir à chaque type de flux une certaine qualité de service. Deux approches de la QoS sont actuellement définies : *Integrated Services* (**IntServ**, RFC 1633) et *Differentiated Services* (**DiffServ**, RFC 2474).

Integrated Services

Le modèle IntServ (Services Intégrés) tend au respect de l'intégrité des flux, c'est une transposition des techniques de **CoS** (*Class of Services*) des réseaux à état dit dur (*hard-state*) tels qu'ATM et Frame Relay. À l'instar de ces protocoles, IntServ définit un état dit mou (*soft-state*) via un protocole de signalisation (**RSVP**, *Resource reSerVation Protocol*). Un réseau à état mou est un réseau qui maintient un contexte durant un certain temps. En l'absence de renouvellement périodique, cet état est détruit. IntServ définit 3 types de service invoqués via le protocole RSVP :

– Un service garanti (*Guaranteed Services*), similaire au service CBR (*Constant Bit Rate*) et VBR-rt (*Variable Bit Rate real-time*) d'ATM ;

– Un service contrôlé (*Controlled Load*) qui correspond au service ABR (*Available Bit Rate*) avec un minimum garanti d'ATM (*guaranteed minimum cell rate*) ;

– Un service *Best Effort*, assimilable à l'UBR (*Unspecified Bit Rate*) d'ATM.

RSVP reste dans la philosophie du protocole IP. En effet, si RSVP permet de décrire un état dans un routeur (*soft-state*), il ne crée pas pour cela une connexion (*hard-state*). Si le réseau n'a pas la capacité de garantir la qualité de service invoquée ATM ou Frame Relay refusent la connexion, ce n'est pas le cas de RSVP, le flux sera traité en *best effort*. La figure 14.44 illustre le principe de RSVP. La source (A) émet un message contenant les références du flux (adresse IP source et destination, port source et destination, protocole), un contexte d'acheminement est mémorisé (message RSVP *Path*) mais aucune ressource n'est allouée. Elles le seront par le destinataire (B) dans un message de réponse RSVP *Resv*.

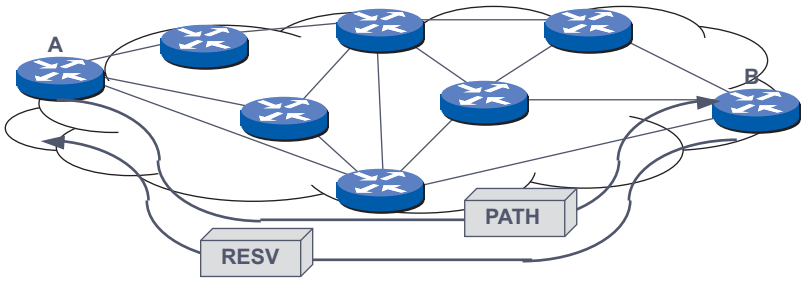


Figure 14.44 La réservation de ressources sous RSVP.

L'approche *Integrated Services* peut être considérée comme une adaptation dans le mode datagrammes des techniques orientées connexion. Chaque application formule une demande de réservation de ressources de bout en bout. Le modèle IntServ et RSVP, compte tenu de sa complexité, n'a connu aucun succès.

© Dunod – La photocopie non autorisée est un délit

Differentiated Services

L'approche DiffServ (Services Différenciés) est plus conforme à l'approche IP. DiffServ implémente un mécanisme de partage de bande passante en introduisant la notion de politique d'acheminement en fonction d'une classe de service (RFC 2474, *Differentiated Service* ou *Diffserv*). Les flux ne sont plus traités individuellement comme dans IntServ, mais ils sont attribués à une classe de service identifiée par un champ spécifique *Differentiated Services Field* (DSF). Tous les flux d'une même classe sont traités de la même façon dans le réseau. Le champ DiffServ remplace le champ TOS d'IPV4 et le champ Classe de Servive d'IPV6. La figure 14.45 rappelle la structure de chacun de ces champs.

Diffserv répartit le trafic en trois classes de service (COS, *Class Of Service*) :

– *Assured Forwar*ding ou *Olympic Service* (RFC 2597), équivalent des services ABR d'ATM, comporte 4 classes, elles-mêmes subdivisées en fonction d'une politique d'écartement (**RED**, *Random Early Drop*) en fonction de l'état du réseau (*Low Drop*, *Medium Drop* et *High Drop*). À chaque classe sont affectées une priorité et une garantie de bande passante.

– *Expedited Forwarding* ou *Premium Service* (RFC 2598), équivalent aux services CBR et VBR-rt d'ATM et défini spécifiquement pour les applications temps réel, minimise le temps de latence dans le réseau. Celui-ci prend en compte des contraintes fortes en matière de temps de traversée, de variation de celui-ci (gigue) et de pertes de données. L'utilisation de la classe *Premium* doit être limitée au sein du réseau, un abus d'utilisation peut fortement pénaliser les autres types de trafic.

– *Best Effort*, équivalent du service UBR d'ATM, correspond au trafic traditionnel sur IP sans qualité de service.

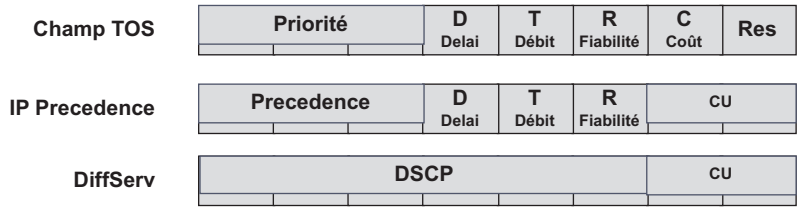


Figure 14.45 Les champs TOS, IP Precedence et DiffServ.

La classification et la vérification des flux sont effectuées à la périphérie du réseau (*Classifier*). Les propriétés du flux sont ensuite analysées (*Metering* ou dimensionnement) en fonction d'un contrat de service préétabli (**SLA**, *Service Level Agreement*). Les datagrammes sont alors marqués (*Marker*) par positionnement du champ **DS Field**. Le trafic différentié ou colorisé (*Multiflow Classifier*) est analysé, certains paquets peuvent être retardés (mise en forme du trafic ou *shaper*) voire éliminés pour prévenir un éventuel état de congestion (*Dropper*). Les paquets sont ensuite affectés à une file d'attente spécifique avant d'être transmis sur le réseau (*Forwarding*). La figure 14.46 illustre les mécanismes que nous venons de décrire.

L'architecture DiffServ est bien adaptée aux grands réseaux. En effet, les classes de services étant attribuées en périphérie du réseau DiffServ, elles ne génèrent ni trafic de gestion, ni surcharge CPU. Cependant, si DiffServ permet de hiérarchiser les flux, il ne dispose pas de mécanisme d'information d'état du réseau. De ce fait, les routeurs de bordures ne sont pas en mesure d'anticiper et ni de réagir à un état de précongestion ou de congestion.

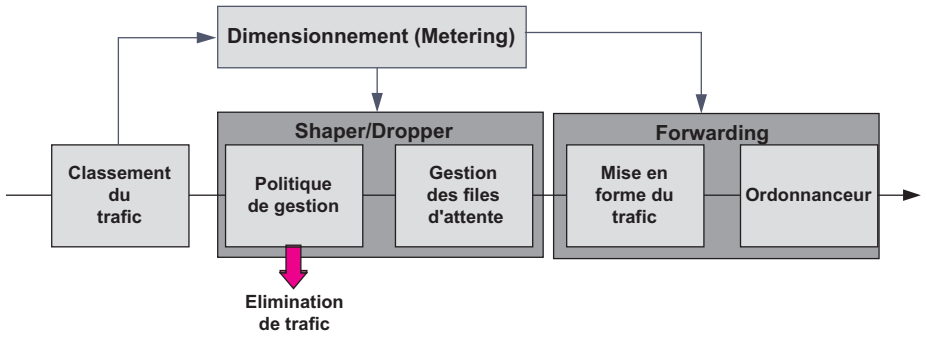


Figure 14.46 Mécanismes de QoS sous DiffServ.

Dans un environnement multi-opérateur, le contrat, négocié avec son opérateur local (SLA) n'est pas connu des opérateurs de réseaux de transit. En principe, chaque domaine DiffServ est indépendant et gère les classes de service selon sa propre politique. Dans ces conditions, DiffServ ne peut garantir une QoS de bout en bout !

La QoS vue par les constructeurs

Devant le besoin croissant de qualité de service, et notamment dans les réseaux privés, les constructeurs ont tous implémenté dans leurs équipements des mécanismes de QoS plus ou moins proches des solutions retenues par l'IETF et notamment de DiffServ. La figure 14.47 illustre une telle réalisation.

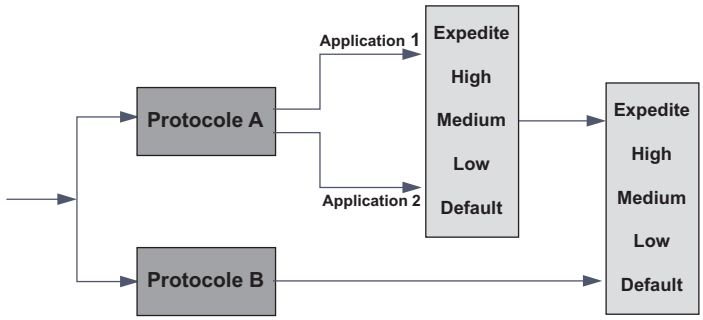


Figure 14.47 Principe de la prioritisation de protocole.

L'attribution de tel ou tel type de flux à une file d'attente de priorité donnée peut combiner plusieurs critères. Ainsi, dans le modèle représenté figure 14.47, le critère premier est le protocole (TCP, UDP...), mais après un premier classement des flux, un second critère de sélection peut être retenu comme dans l'exemple de la figure 14.47, l'application. La sélection sur numéro de port (application) peut être statique (port réservé) ou, pour distinguer deux applications de même nature (deux flux Telnet par exemple), attribuée dynamiquement (port éphémère).

Cependant, la gestion de la QoS ne crée pas de bande passante, la stratégie d'attribution d'un niveau de priorité ou d'une partie de la bande passante à tel ou tel flux doit être étudiée avec beaucoup d'attention. La figure 14.48 illustre un tel système de qualité de service.

Dans le système de la figure 14.48, les flux sont acheminés en fonction de deux politiques de gestion de la priorité. La première dite *Priority Based Forwarding* est attribuée aux flux qui

© Dunod – La photocopie non autorisée est un délit

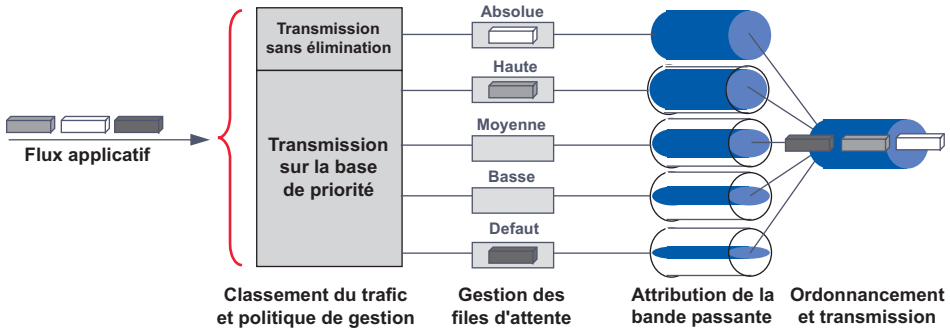


Figure 14.48 Routage fondé sur la notion de priorité.

ne doivent subir aucun retard, toute la bande passante du système leur est attribuée (administration du réseau, voix). Dans la seconde, dite *Credit Based Wait and Forwarding* si des flux plus prioritaires doivent être écoulés, ces flux sont éventuellement mis en attente. C'est l'administrateur réseau qui définit, lors de la configuration du système, les critères d'affectation à tel ou tel type de traitement et qui alloue toute ou partie de la bande passante à telle ou telle file d'attente.

Conclusion

Le véritable problème de la qualité de service réside dans la garantie de celle-ci de bout en bout. Or, compte tenu des différentes implémentations des constructeurs, des différentes approches des instances de normalisation et de la liberté de choix de chaque opérateur sur la politique de qualité de service qu'il intègre à son réseau, celle-ci ne peut valablement être garantie que pour des mises en relation qui restent dans le domaine d'un même opérateur.

14.4.4 Routage multicast

Introduction au multicast

L'IP multicast est un mécanisme qui permet de diffuser des datagrammes IP vers un ou plusieurs récepteurs sans que ces datagramme soient adressés individuellement à chaque hôte. Les nœuds destination sont identifiés par une adresse de groupe (adresse multicast). Cette technique évite l'envoi de N datagrammes unicasts aux N clients d'une même source d'information.

Dans l'exemple de la figure 14.49, un serveur d'applications vidéo (serveur multicast) est raccordé à un réseau IP multicast. Pour recevoir les émissions, les machines distantes doivent, au préalable, s'abonner au serveur vidéo. Le mécanisme d'abonnement est spécifique au logiciel serveur, il n'entre pas dans le cas de notre étude. Les machines abonnées sont membres du groupe multicast. Une machine peut être membre de plusieurs groupes. Les informations ne sont diffusées sur les brins locaux que si au moins une machine locale s'est abonnée à un service multicast. Dans notre exemple, un seul exemplaire du datagramme est diffusé sur le réseau multicast, chaque routeur ayant un client abonné rediffuse le datagramme sur le brin local auquel il est raccordé. Les informations vidéo ne sont pas diffusées sur le troisième réseau où aucune machine n'a rejoint un groupe de multicast.

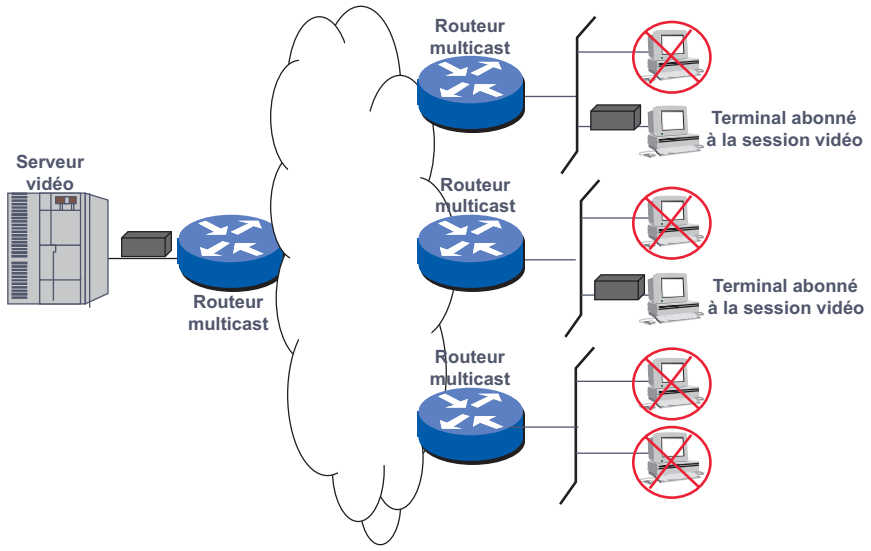


Figure 14.49 Principe d'un réseau multicast.

La diffusion multicast nécessite deux protocoles. Le premier doit permettre au routeur local d'apprendre s'il a, sur son brin local, des clients multicast, le second doit assurer un routage minimal dans le réseau WAN.

Rappel sur l'adressage multicast

L'adressage multicast doit garantir qu'un seul message est diffusé sur le réseau, qu'un client multicast peut être localisé (@IP multicast) et que la station puisse distinguer les messages qui lui sont destinés (@MAC multicast).

Des adresses IP multicast (classe D) ont été définies pour permettre de distinguer le groupe multicast de rattachement. Les applications multicast fournissent au coupleur (NIC) les adresses MAC multicast auxquelles il doit répondre. Ces adresses sont construites à partir des adresses IP multicast. Les adresses MAC multicast s'étendent de :

01-00-5E-00-00-00 à 01-00-5E-7F-FF-FF (RFC 1112).

La figure 14.50 indique comment, à partir de l'adresse IP multicast de la station, est construite l'adresse MAC multicast. Les 5 bits de l'adresse IP non utilisés pour former l'adresse MAC permettent, éventuellement, de distinguer 32 groupes multicast sur une même adresse MAC multicast.

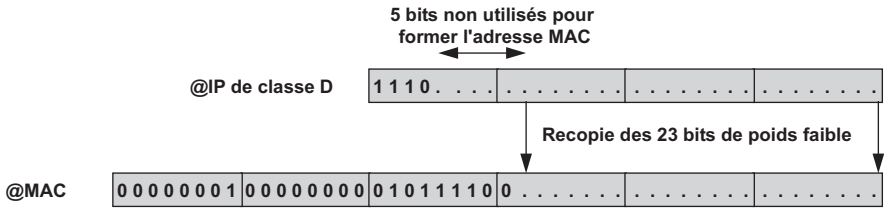

5 bits non utilisés pour
former l'adresse MAC
@IP de classe D
1 1 1 0 . . . .
Recopie des 23 bits de poids faible
@MAC
0 0 0 0 0 0 0 1
0 0 0 0 0 0 0 0
0 1 0 1 1 1 1 0
0 . . . . . .

Figure 14.50 Mappage @IP et @IEEE multicasts.

© Dunod – La photocopie non autorisée est un délit

Les adresses de groupe les plus connues sont :

– 224.0.0.1, tous les hôtes multicast de ce sous-réseau ;
– 224.0.02, tous les routeurs multicast de ce sous-réseau ;
– 224.0.0.4, tous les routeurs exécutant le protocole de routage multicast DVMRP ;
– 224.0.1.11, applications audio (IETF) ;
– 224.0.1.12, application vidéo (IETF) ;
– 224.0.1.16, diffusion de musique (Music-Service) ;
– 224.0.1.17, *Audionew* (bulletins d'information radio) ;

Le protocole local IGMP (RFC 2236)

Le protocole **IGMP** (*Internet Group Management Protocol*) est le protocole d'apprentissage utilisé par les routeurs multicast pour découvrir l'existence, dans les sous-réseaux auxquels ils sont raccordés, de membres d'un groupe multicast (figure 14.51).

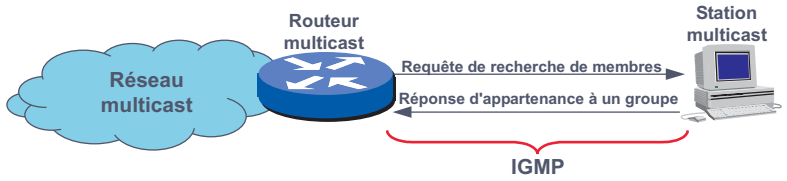


Figure 14.51 Principe du protocole IGMP.

Le protocole IGMP version 2 utilise quatre types de messages et un seul format (figure 14.52) :

– Les messages de demande d'adhésion (*Host Membership Query*, type = 0x11) destinés à demander régulièrement aux stations à quel groupe multicast elles appartiennent. Un seul routeur multicast du réseau envoie régulièrement ces messages (routeur dominant), c'est celui de plus petite adresse IP. Le champ *Multicast Group Address* est à 0.
– Les messages de réponse (*Host Membership Report*, type = 0x16) sont envoyés par tout hôte appartenant à un groupe de diffusion multicast. Chaque hôte répond après un délai aléatoire avant le délai imposé (*Max response Time*). Le champ *Multicast Group Address* est alors renseigné sur le groupe d'appartenance. Si un hôte a déjà répondu pour ce groupe, les autres hôtes du même groupe s'abstiennent alors de répondre.
– Lorsqu'un hôte quitte une session multicast, il envoie un message d'abandon de groupe (*Leave Group Message*, type 0x17) à l'adresse multicast 224.0.0.2 (tous les routeurs multicast du sous-réseau).
– En réponse à ce message, le routeur demandeur envoie un message de demande d'adhésion spécifique au groupe qui vient d'être quitté (*Group Specific Query Message*, type = 0x11 mais avec le champ *Multicast Group Address* renseigné du groupe multicast abandonné). En l'absence de réponse, le groupe est supprimé de sa liste d'adhésion et plus aucun message concernant ce groupe ne sera relayé sur le sous-réseau.

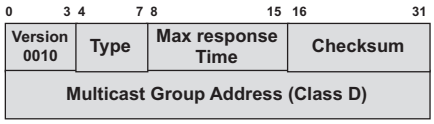


Figure 14.52 Format des messages IGMP.

Le protocole de routage multicast DVMRP (RFC 1075)

➤ Concepts du routage multicast

IGMP assure la diffusion des datagrammes multicast à l'ensemble des stations d'un sous-réseau local. Cependant, dans le réseau (Internet ou autre), le routage des datagrammes multicast doit être assuré de manière à économiser la bande passante. Plusieurs mécanismes peuvent être mis en œuvre :

– le *Floding* ou inondation, très facile à mettre en œuvre puisque le routeur n'a aucune table d'acheminement à entretenir, mais cette méthode génère un trafic d'autant plus important que le réseau est grand ;

– le *Spanning Tree* permet de construire un chemin unique (arbre) entre une source (racine) et une destination (feuille) ;

– le *Reverse Path Broadcasting* (**RPB**) aussi appelé *Reverse Path Forwarding* est une amélioration des performances du *Spanning Tree*. RPB construit un arbre par groupe de multicast. Le principe est relativement simple quand un routeur reçoit un paquet sur une interface, il examine si l'interface d'arrivée est bien sur le chemin le plus court pour rejoindre la source (celle qui serait utilisée pour envoyer un datagramme unicast à la source). Si c'est le cas, le paquet est diffusé sur toutes les autres interfaces du routeur (inondation), sinon le paquet est détruit.

➤ Le protocole DVMRP (Distance Vector Multicast Routing Protocol, RFC 1075)

DVMRP est un protocole vecteur distance destiné à assurer le routage multicast. Une variante de l'algorithme *Reverse Path Brocasting* est utilisée pour construire les tables de routage multicast. DVMRP est le complément réseau du protocole local IGMP (figure 14.53).

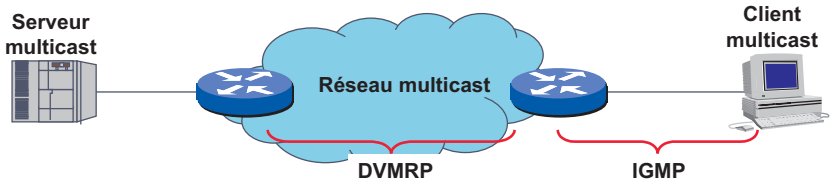


Figure 14.53 Complémentarité des protocoles IGMP et DVMRP.

L'arbre multicast établit des relations en « amont » et en « aval » entre les différents routeurs du réseau. L'arbre de diffusion est maintenu à jour selon une méthode dite élagage et greffe. Lorsqu'un routeur multicast n'a plus d'abonné pour un groupe (hôte final ou routeur aval), il émet un message dit *prune packet* pour informer en amont de l'inutilité de maintenir un lien de diffusion multicast pour ce groupe (élagage de la branche). Le routeur ne supprimera cette route qu'à l'échéance d'un timer. À l'inverse à la réception d'une demande d'adhésion, il émet un message dit *graft packet* pour reconstruire une route vers la source (greffe). Ce fonctionnement est illustré figure 14.54.

© Dunod – La photocopie non autorisée est un délit

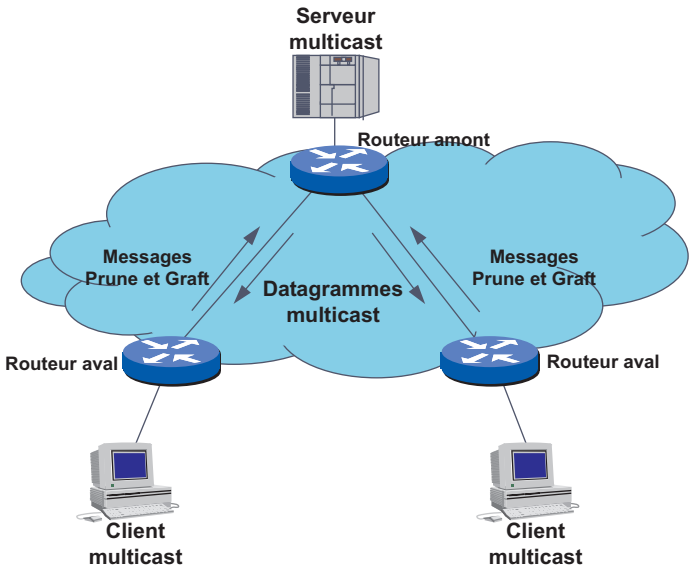


Figure 14.54 Diffusion de messages dans un réseau DVMRP.

À l'instar de RIP, le protocole DVMRP échange ses tables de routage avec ses voisins DVMRP (message *route report* toutes les 60 s à l'adresse de diffusion 224.0.0.4). Les voisins DVMRP sont découverts par l'émission, toutes les 10 s, de messages *probe message*.

➤ Internet et le multicast

La composante d'Internet qui assure la diffusion de messages en multicast sur le réseau est désignée sous le nom de **Mbone** (*Multicast Backbone*). Il s'agit d'un réseau virtuel reliant les différents routeurs multicast (mrouteurs) par des tunnels (tunnels multicast), mais le service rendu est du type datagramme.

Diverses applications sont offertes téléconférences, programmes radio, jeux... Un annuaire des sessions en cours permet aux utilisateurs de rejoindre un groupe de diffusion.

14.4.5 Fonctions annexes des routeurs

Les routeurs multiprotocoles

Dans des environnements complexes, il arrive que plusieurs protocoles réseaux soient utilisés en même temps (IP, IPX...). Les routeurs capables d'assurer l'acheminement de données de différents protocoles sont dits routeurs multiprotocoles.

Dans ces environnements, se pose la question de la reconnaissance du protocole à router. Digital, Intel et Xerox ont résolu ce problème en introduisant dans la trame Ethernet (Ethernet V2) le champ type de protocole (*Ethertype*). ISO identifie le protocole supérieur par les champs DSAP et SSAP de la trame LLC. Certaines implémentations de réseaux locaux utilisent la trame LLC mais des protocoles de niveau supérieur non ISO (Token Ring...). Pour résoudre le problème d'identification, une encapsulation supplémentaire a été introduite : l'encapsulation **SNAP** (*SubNetwork Access Protocol*). La figure 14.55 rappelle ces différents formats pour les réseaux de type Ethernet.

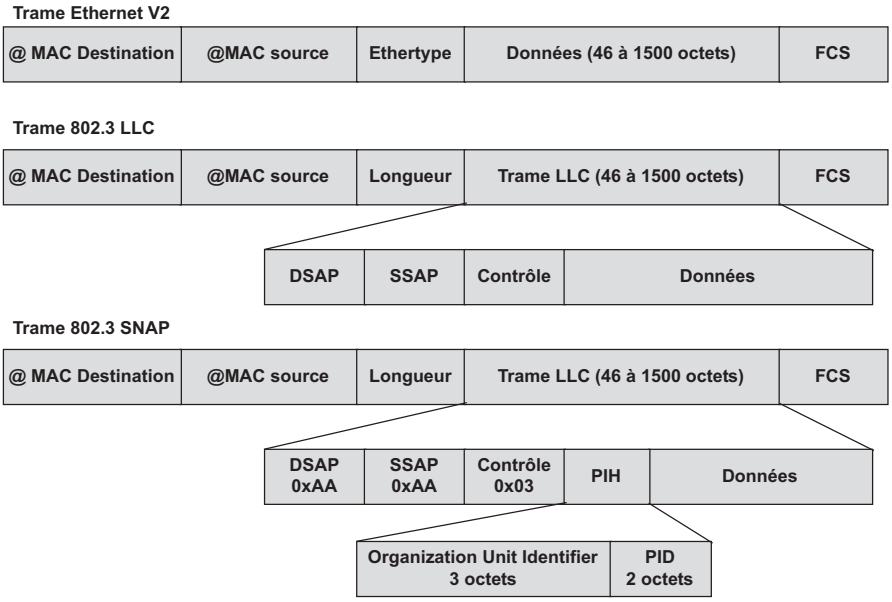


Figure 14.55 L'encapsulation SNAP.

À la réception d'une trame Ethernet, le routeur examine le champ Type, si la valeur est supérieure à 1 500, la trame est au format Ethernet V2, et le champ contient l'Ethertype du protocole transporté. Si la valeur est égale ou inférieure à 1 500 la trame est au format IEEE 802.3, le protocole supérieur est alors identifié par les champs SSAP et DSAP de la trame LLC (codage ISO). Si la valeur contenue dans ces champs est « 0xAA », la trame LLC encapsule une trame SNAP et le protocole est identifié par le champ **PIH** (*Protocol Identification Header*) dans le sous-champ **PID** (*Protocol_ID*) dont le codage correspond à celui du champ Type de la trame Ethernet V2.

Le sous-champ **OUI** (*Organization Unit Identifier*, 3 octets) contient l'identification du constructeur de la carte transporteur, c'est le code IEEE du fournisseur, il peut aussi désigner un organisme de normalisation (par exemple la valeur 0x00-80-C2 désigne l'IEEE 802.1). Ce champ est mis à zéro (0x00-00-00) pour les trames Ethernet V2.

La compression de données

Afin d'optimiser l'utilisation des liens, certains routeurs (et les ponts distants) utilisent la compression de données. Trois modes de compression sont généralement offerts :

– la compression des en-têtes (*header*),

– la compression du champ données seul (*payload*),

– la compression de la trame complète (*link*).

La compression des en-têtes n'est intéressante dans le monde IP que si les paquets de données sont de très petites tailles (terminal Telnet, par exemple). La compression du champ données seul semble la solution la plus efficace. En effet, le champ en-tête non compressé optimise les performances des routeurs intermédiaires qui n'ont pas besoin de décompresser la trame entière ou l'en-tête pour router correctement le paquet. Certains routeurs activent ou

© Dunod – La photocopie non autorisée est un délit

désactivent dynamiquement la compression en fonction de la nature des données à transmettre (données déjà compressées).

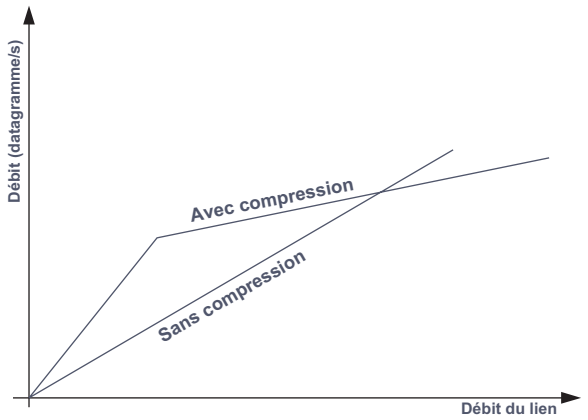


Figure 14.56 Efficacité de la compression en fonction du débit du lien.

La compression de données n'est utile que si le temps réel d'émission des données compressées est inférieur au temps d'émission des données non compressées. À partir d'un certain débit du lien, la compression pénalise le temps d'émission (temps CPU). Dans ce cas, la compression ne présente un intérêt que si on utilise un réseau facturé au volume (figure 14.56).

*Le routage à la demande (*Dial on Demand*)*

Le routage à la demande est une technique mise en œuvre dans les petits routeurs (routeurs d'agence) n'ayant aucun lien permanent avec le réseau, le *Dial on Demand* établit un lien commuté (RTC ou RNIS) lorsque des données sont à transmettre (figure. 14.57).

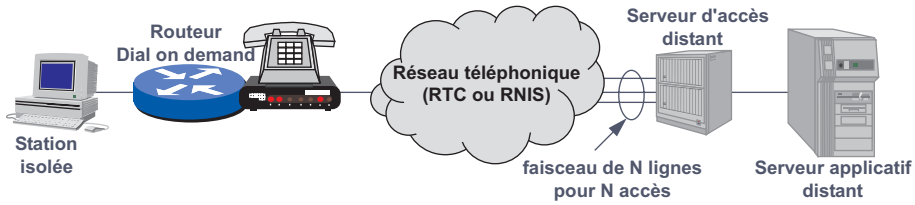


Figure 14.57 Principe du *Dial on Demand*.

Pour éviter les reconnexions successives, la connexion n'est rompue qu'à l'échéance d'un timer (*Idle Timer*). Le serveur distant authentifie l'appelant par son numéro d'appelant ou un mot de passe de connexion.

*Bande passante à la demande (*Bandwith on Demand*)*

Ce service, similaire au précédent, établit une connexion (lien de débordement) avec un réseau numérique (RNIS) dès qu'un certain seuil (*Threshold*) de trafic, mesuré par la taille des files d'attente, est atteint sur le lien principal. La connexion est rompue dès que le trafic redescend en dessous de ce seuil (figure 14.58).

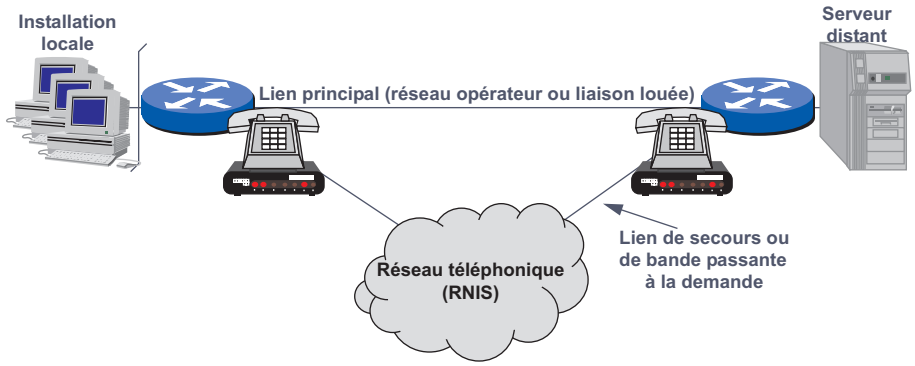

Installation locale
Serveur distant
Lien principal (réseau opérateur ou liaison louée)
Réseau téléphonique (RNIS)
Lien de secours ou de bande passante à la demande

Figure 14.58 Principe du *Bandwith* on *Demand*.

Le *Bandwith on Demand* ou bande passante à la demande peut utiliser plusieurs canaux B. Cette même technique permet d'utiliser le réseau RNIS en cas de défaillance totale du lien principal (lien de secours).

Comparaison entre les ponts et les routeurs

Indépendamment du facteur coût, ponts et routeurs diffèrent essentiellement par leur performance intrinsèque, le niveau de sécurité qu'ils autorisent et leur facilité de mise en œuvre.

➤ Comparaison en termes de performance

Les ponts agissant au niveau 2 sont, de ce fait, plus efficaces (moins de temps de traitement). Essentiellement recommandés dans les environnements Ethernet en raison de leur faculté à isoler le trafic, ils sont aujourd'hui avantageusement remplacés par les commutateurs.

Cependant, tous les protocoles réseaux utilisent de nombreux messages de diffusion (broadcast), les ponts (commutateurs) ne peuvent filtrer ces messages, les routeurs peuvent les filtrer. Dans une configuration utilisant des liens distants, donc à faible débit vis-à-vis du débit sur le LAN, la diffusion consomme une part importante de la bande passante. L'usage des ponts est donc à réserver à l'interconnexion locale.

➤ Comparaison en termes de sécurité

La sécurité réalisée au niveau applicatif par de simples mots de passe est insuffisante au niveau d'un réseau. Il est nécessaire d'interdire les pénétrations sur le réseau lui-même. Il est évidemment possible de réaliser des filtres sur adresse MAC, mais il est alors nécessaire d'introduire soit la totalité des adresses autorisées, soit la totalité des adresses interdites !

Sur les routeurs, le filtre peut être défini par un ensemble d'adresses IP, ou, à l'aide du masque de sous-réseau, sur la totalité du trafic d'un sous-réseau, ce qui est évidemment plus facile. Certains routeurs peuvent effectuer de véritables translations d'adresses masquant ainsi au monde extérieur les adresses réelles utilisées localement.

➤ Comparaison en termes de facilité de mise en œuvre

Les ponts sont transparents aux protocoles de niveau supérieur, ils ne nécessitent aucune configuration particulière.

© Dunod – La photocopie non autorisée est un délit

➤ Les bridges routeurs (B-routeurs)

La plupart des constructeurs ont développé, dans un même châssis les fonctionnalités des ponts (niveau 2) et des routeurs (niveau 3). Lors de la réception d'une trame, ces équipements examinent son contenu. S'il reconnaît un protocole routable (IP, IPX...) la trame est traitée par l'entité routeur. Si le protocole acheminé n'est pas routable (exemple NetBIOS), la trame est alors pontée.

Les ponts/routeurs ou B-Routeurs sont utilisés dans les environnements multiprotocoles et dans les réseaux en phase de migration d'un protocole de type NetBIOS, protocole non routable vers un protocole routable.

14.5 LES PASSERELLES APPLICATIVES

Les passerelles mettent en relation des systèmes totalement hétérogènes. Elles réalisent une adaptation des protocoles telle qu'une application d'un environnement A voit l'application distante de l'environnement B, comme si celle-ci appartenait au monde A.

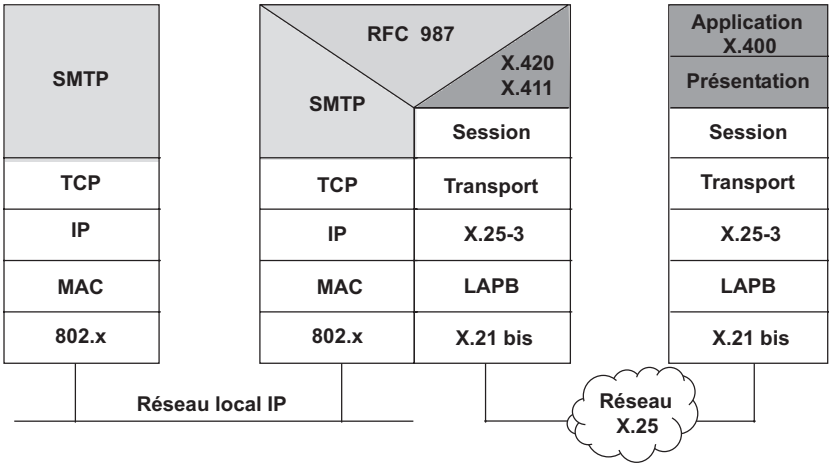


Figure 14.59 Exemple de passerelle applicative

La figure 14.59 représente une passerelle entre une messagerie ISO X.400 et la messagerie **SMTP** (*Simple Mail Transfer Protocol*) du monde Internet.

EXERCICES

Exercice 14.1 Interconnexion d'un réseau 802.3 et 802.5

Vous envisagez de réaliser un pont susceptible d'interconnecter un réseau 802.3 avec un réseau 802.5. Quels sont les problèmes à résoudre ?

Exercice 14.2 Spanning tree

Construisez l'arbre recouvrant (*spanning tree*) du réseau de la figure 14.60 en prenant en compte les identifiants (ID) et les coûts (C) indiqués. Commentez la solution obtenue, en existe-t-il une meilleure ?

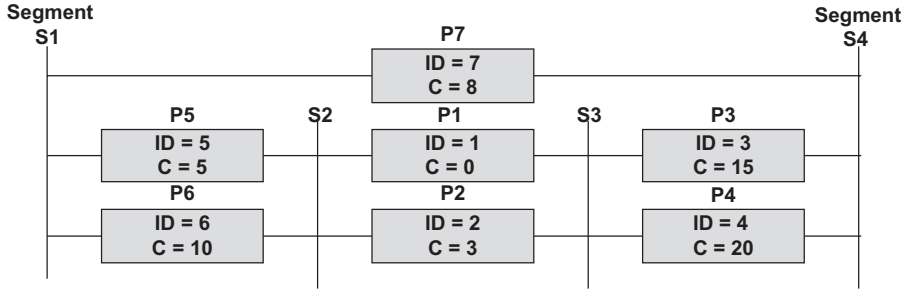


Figure 14.60 Réseau ponté avec chemins redondants.

Exercice 14.3 Protocole RIP/OSPF

Compléter le tableau suivant (figure 14.61) :

	RIP	OSPF
Caractéristiques		
Type d'algorithme		
Métrique		
Métrique configurable		
Origine		
Architecture du réseau		
Type		
Nombre de routeurs		
Routeur maître		
Support des masques de longueur variable		
Performance		
Charge du réseau		
Périodicité des mises à jour		
Temps de convergence		
Mode de mise à jour		
Support de la qualité de service		
Sécurité		
Authentification		

Figure 14.61 Comparaison RIP/OSPF.

© Dunod – La photocopie non autorisée est un délit

Exercice 14.4 Agrégation de routes

Supposons le réseau de la figure 14.62. Les trois aires raccordées à la zone backbone utilisent des adresses privées 10.0.0.0. Chaque aire peut comporter jusqu'à 16 sous-réseaux terminaux. Les adresses de sous-réseaux et les masques associés sont indiqués sur la figure. On vous demande :

a) Quel serait, en l'absence d'agrégation d'annonces, le nombre d'entrées dans la table du routeur de bordure d'aires du backbone ?

b) Quelles adresses et quels masques annoncent les routeurs de bordure d'aires ?

c) Dans quel ordre les adresses seront inscrites dans la table du routeur de bordure de l'aire backbone ?

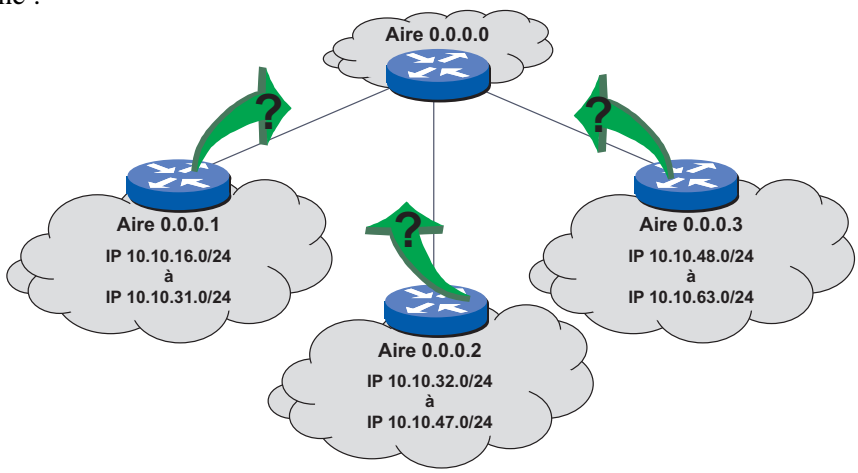


Figure 14.62 Réseaux OSPF.

Exercice 14.5 Adresses multicast

Un groupe multicast est identifié par l'adresse IP multicast 224.16.21.5. À quelles adresses MAC répondra l'adaptateur Ethernet d'adresse unicast 08-00-02-2D-75-BD situé sur le sous-réseau 10.10.31.0/24 ?

Exercice 14.6 Comparaison pont/routeur

Compléter le tableau suivant (figure 14.63) :

	Pont	Routeur
Configuration		
Transparence aux protocoles		
Sécurité (Filtre)		
Extension du réseau		
Trafic de service		
Broadcast		
Charge de travail (personnel)		

Figure 14.63 Comparaison Pont/Routeur.

Exercice 14.7 Masque de sous-réseau

Deux réseaux (A et B) utilisent le protocole TCP/IP, ils sont reliés via un routeur. L'entreprise a défini le masque de sous-réseau : 255.255.0.0. Un utilisateur du réseau A sur la machine 100.64.0.102 se plaint de ne pouvoir joindre un correspondant d'adresse 100.64.45.102 du réseau B. Expliquez pourquoi, donnez une solution simple pour que ces machines puissent communiquer ?

Exercice 14.8 Routage statique

En reprenant le plan d'adressage de la solution de l'exercice 12.11, établissez les tables de routage (routage fixe) du réseau. Pour répondre aux Ping, les adresses des LL (liaisons louées) seront incluses dans les tables. Vous vous aiderez de la figure 14.64 ci-dessous.

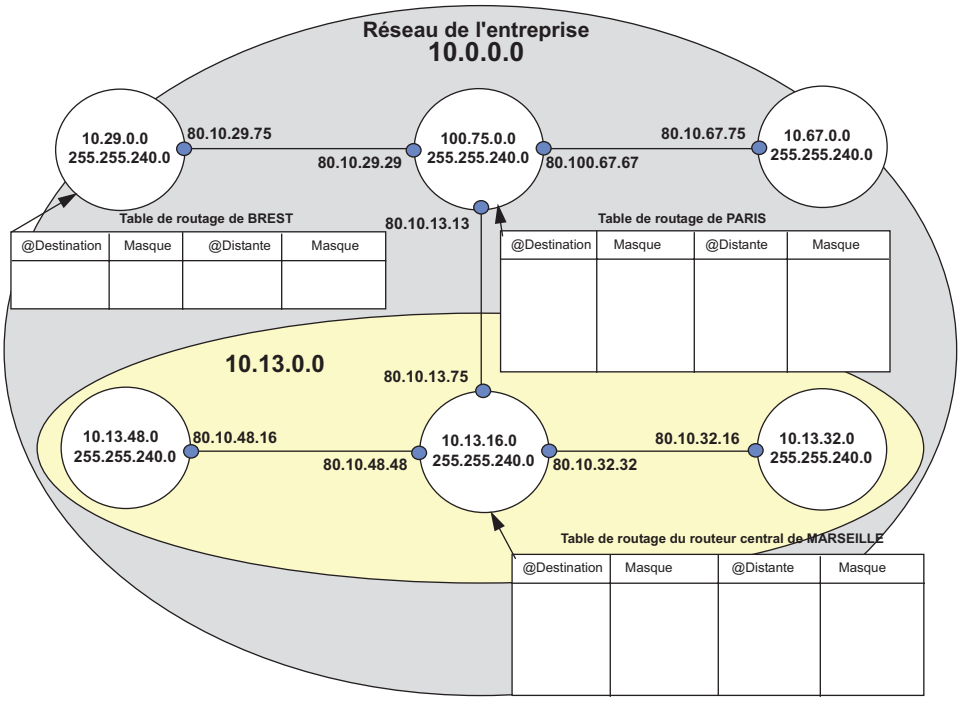


Figure 14.64 Plan d'adressage et tables de routage du réseau 10.0.0.0.

© Dunod – La photocopie non autorisée est un délit

Chapitre **15**

La téléphonie

15.1 PRINCIPES GÉNÉRAUX DE LA TÉLÉPHONIE

Le transport de la voix est historiquement à l'origine des premiers réseaux de transmission. Le réseau téléphonique public **RTPC** (Réseau Téléphonique Public Commuté ou simplement **RTC**) ou encore **PSTN** (*Public Switched Telecommunication Network*) a essentiellement pour objet le transfert de la voix. En France, le transport des données n'y est autorisé que depuis 1964. Utilisant le principe de la commutation de circuits, le réseau téléphonique met en relation deux abonnés à travers une liaison dédiée pendant tout l'échange (figure 15.1).

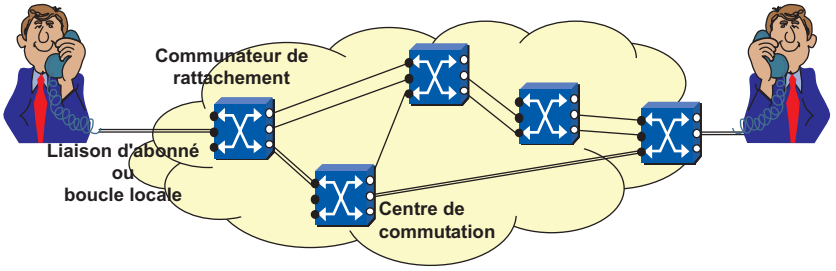


Figure 15.1 Principe du réseau téléphonique commuté.

À l'origine, la mise en relation était réalisée manuellement par des opérateurs[1]. Bien que les premiers concepts de commutation automatique apparurent en 1889, ce n'est qu'en 1970 que le réseau téléphonique français fut entièrement automatisé.

1. La petite histoire rapporte que le premier commutateur téléphonique automatique a été imaginé par Strowger (1889) pour lutter contre son concurent commercial (service de pompes funèbres) dont l'épouse était opératrice au centre téléphonique local (Kansas City aux Etats-Unis) et qui acheminait les appels à destination des pompes funèbres vers l'entreprise de son mari !

La commutation de circuits ou commutation spatiale consiste à juxtaposer bout à bout des voies physiques de communication, la liaison étant maintenue durant tout l'échange. La numérisation de la voix a permis le multiplexage temporel des communications. La commutation spatiale a été remplacée par la commutation d'intervalles de temps (IT) ou commutation temporelle. Ce concept est illustré figure 15.2. En mettant en relation un IT d'une trame en entrée avec un IT d'une autre trame en sortie, la commutation temporelle émule un circuit. La communication est *full duplex*, une bande passante de 64 kbit/s, dans chaque sens, est donc réservée durant toute la communication.

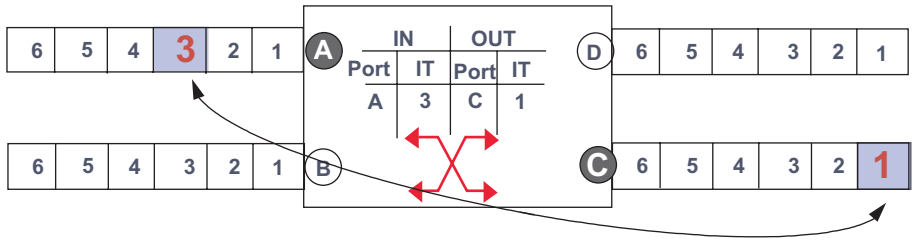


Figure 15.2 Principe de la commutation temporelle.

Les supports de transmission sont constitués de voies numériques multiplexées selon une hiérarchie appelée hiérarchie plésiochrone (*Plesiochronous Digital Hierarchy*, **PDH**). Malgré la numérisation du réseau, la liaison des abonnés résidentiels est restée essentiellement analogique. C'est le commutateur de rattachement qui réalise la fonction de numérisation et de dénumérisation de la voix (figure 15.3).

Figure 15.3 Les modes de raccordement.

15.2 ORGANISATION DU RÉSEAU TÉLÉPHONIQUE

15.2.1 Architecture traditionnelle

Le réseau téléphonique a une organisation hiérarchique à trois niveaux (figure 15.4). Il est structuré en zones, chaque zone correspond à un niveau de concentration et en principe de taxation. On distingue :

– Zone à Autonomie d'Acheminement (**ZAA**), cette zone, la plus basse de la hiérarchie, comporte un ou plusieurs Commutateurs à Autonomie d'Acheminement (**CAA**) qui eux-mêmes desservent des Commutateurs Locaux (**CL**). Les commutateurs locaux ne sont que de simples concentrateurs de lignes auxquels sont raccordés les abonnés finals. La

ZAA (Zone à Autonomie d'Acheminement) est un réseau étoilé, elle constitue le réseau de desserte ;

– Zone de Transit Secondaire (**ZTS**), cette zone comporte des Commutateurs de Transit Secondaires (**CTS**). Il n'y a pas d'abonnés reliés directement aux CTS (Commutateurs de Transit Secondaires). Le réseau étant imparfaitement maillé lorsqu'un CAA (Commutateur à Autonomie d'Acheminement) ne peut atteindre directement le CAA destinataire, ils assurent le brassage des circuits ;
– Zone de Transit Principal (**ZTP**), cette zone assure la commutation des liaisons longues distances. Chaque ZTP (Zone de Transit Principal) comprend un Commutateur de Transit Principal (**CTP**). Au moins un Commutateur de Transit Principal (**CTP**) est relié à un Commutateur de Transit International (**CTI**).

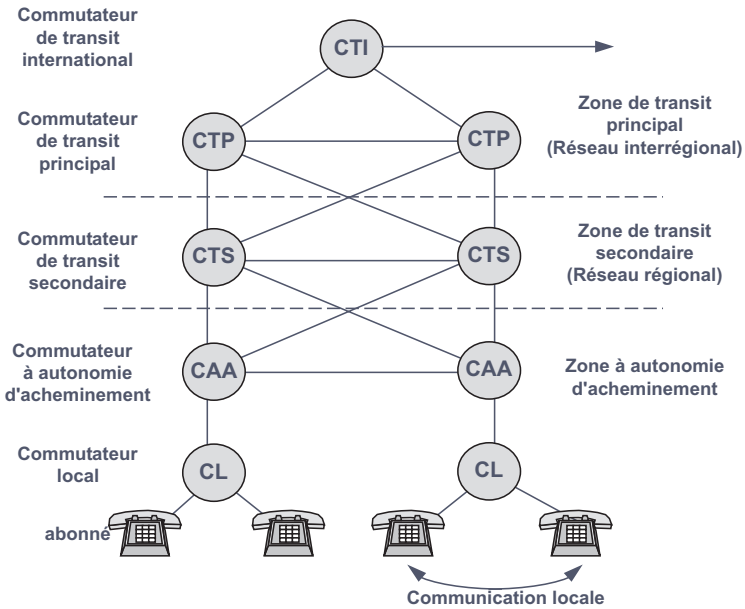


Figure 15.4 Organisation du réseau téléphonique.

Le réseau étant partiellement maillé, plusieurs itinéraires sont généralement possibles pour atteindre un abonné. Afin d'optimiser l'utilisation des faisceaux, on distingue deux types de faisceaux : les faisceaux de premier choix et les faisceaux de second choix ; les faisceaux de second choix constituent des faisceaux de débordement. Pour un numéro donné, le faisceau de premier choix est choisi de telle manière qu'il conduise l'appel vers le commutateur le plus proche de l'abonné appelé en empruntant les faisceaux de plus faible hiérarchie.

15.2.2 Gestion du réseau

La gestion générale du réseau discerne trois fonctions :

– **la distribution**, celle-ci comprend essentiellement la liaison d'abonné ou boucle locale (paire métallique) qui relie l'installation de l'abonné au centre de transmission de rattachement. Cette ligne assure la transmission de la voix (fréquence vocale de 300 à 3 400 Hz), de

© Dunod – La photocopie non autorisée est un délit

la numérotation (10 Hz pour la numérotation décimale – au cadran – et 697 à 1 633 Hz pour la numérotation fréquentielle) et de la signalisation générale (boucle de courant, fréquences vocales) ;

– **la commutation**, c'est la fonction essentielle du réseau, elle consiste à mettre en relation deux abonnés, maintenir la liaison pendant tout l'échange et libérer les ressources à la fin de celui-ci. C'est le réseau qui détermine les paramètres de taxation et impute le coût de la communication à l'appelant ou à l'appelé ;
– **la transmission**, c'est la partie support de télécommunication du réseau, cette fonction est remplie soit par un système filaire cuivre, par de la fibre optique ou par des faisceaux hertziens. Aujourd'hui, le réseau français est intégralement numérisé, seule la liaison d'abonné est encore, la plupart du temps, analogique et sur support cuivre, notamment pour les abonnés résidentiels.

15.3 ÉTABLISSEMENT D'UNE COMMUNICATION TÉLÉPHONIQUE

15.3.1 Principe d'un poste téléphonique

Établir une communication téléphonique c'est mettre en relation deux terminaux téléphoniques. Le poste téléphonique doit remplir plusieurs fonctions, chacune est réalisée par un organe spécifique. Le terminal téléphonique élémentaire comporte cinq organes (figure 15.5) :

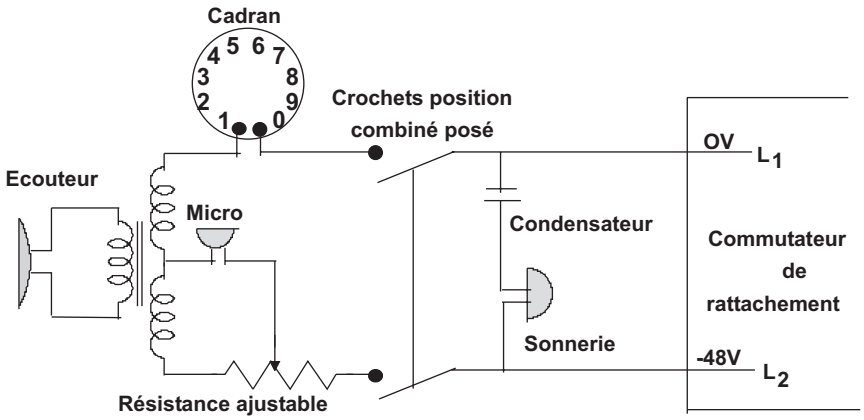


Figure 15.5 Le terminal téléphonique S63.

– les crochets ou supports sur lesquels repose le combiné ; lorsque le combiné est soulevé les contacts se ferment. Le circuit électrique est alors fermé, le commutateur de rattachement détecte le courant et en déduit que l'abonné désire entrer en communication. Un potentiomètre permet d'ajuster ce courant à 30 mA. De même, lors du raccroché, le commutateur détecte l'ouverture de la boucle de courant. L'ouverture ou la fermeture de cette boucle permet, très simplement, au commutateur de rattachement de détecter le changement d'état du terminal (signalisation) ;
– le micro ou capteur, constitué d'une simple membrane qui par ses vibrations, sous l'effet de la pression acoustique (voix), fait varier la résistance interne de celui-ci (micro au charbon).

Ces variations de résistance entraînent des variations du courant dans la boucle de courant. Ce sont ces variations, proportionnelles à la pression sur la membrane (voix), qui constituent le signal analogique de voix transmis, après numérisation, à l'usager distant ;

– un écouteur, membrane métallique qui vibre selon les variations du courant dans le transformateur d'adaptation et restitue le son ;

– un cadran, celui-ci en provoquant l'ouverture de la boucle de courant (numérotation décimale) envoie des impulsions au commutateur. Celles-ci seront interprétées et permettront d'identifier l'appelé ;

– une sonnerie, alimentée en 50 Hz (80 volts), alerte l'abonné distant et l'invite à décrocher, c'est le commutateur de rattachement qui envoie le signal 50 Hz lors d'un appel.

15.3.2 Principe du raccordement d'usager

L'usager est raccordé au réseau via une unité de raccordement (**URA**, Unité de Raccordement d'Abonnés). Celle-ci peut être locale ou distante (**URAD**, Unité de raccordement d'Abonnés Distants). Le commutateur de raccordement assure les fonctions de réception et de mémorisation de la numérotation (Enregistreur), celle-ci est analysée et traduite par un traducteur qui va définir les conditions de taxation et déterminer le routage. Enfin, le sélecteur recherche une ligne disponible (joncteur) et affecte les ressources (circuits ou IT). La figure 15.6 illustre ces différents éléments.

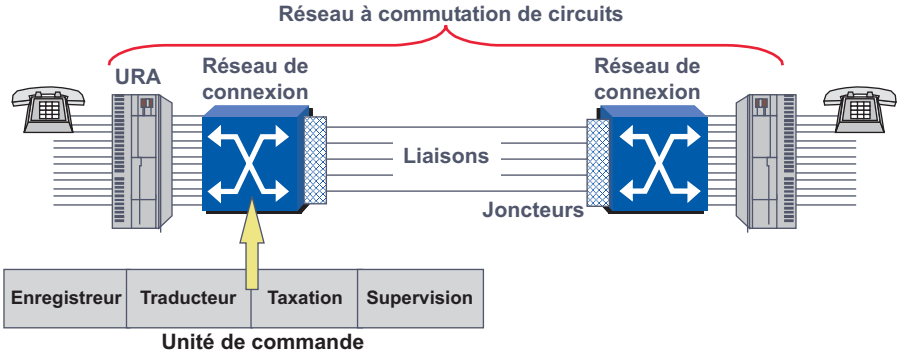


Figure 15.6 Principe du raccordement des abonnés.

15.3.3 La mise en relation Usager/Usager

La mise en relation de deux abonnés répond à un protocole qui organise le dialogue entre les terminaux d'usager et le réseau (signalisation Usager/Réseau). Elle comporte deux ensembles de mécanisme. Le premier correspond à un échange d'information hors communication destiné à établir celle-ci ou à libérer les ressources, c'est la signalisation. Le second est la communication téléphonique proprement dite.

La figure 15.7 illustre les différentes étapes de la mise en relation de deux abonnés, celles-ci au nombre de cinq sont détaillées ci-dessous :

– décroché du combiné, détection de la boucle de courant, envoi de la tonalité d'invitation à numéroter (signal à 440 Hz, le « la » des musiciens) ;

© Dunod – La photocopie non autorisée est un délit

– numérotation, le numéro composé est mémorisé et décodé par le commutateur de rattachement. Le système établit le lien. Durant cet intervalle de temps, le demandeur recevait, avant le 18 octobre 1996, une tonalité dite de progression d'appel[2] ;
– envoi du signal de sonnerie à l'appelé distant et attente du décroché de celui-ci. L'appelant reçoit le signal de retour d'appel communément appelé sonnerie ;
– le correspondant décroche. Le central de rattachement détecte le décroché (boucle de courant), il arrête les signaux de sonnerie, les signaux de retour d'appel et déclenche la taxation ;
– l'échange d'information (voix ou données) peut commencer.

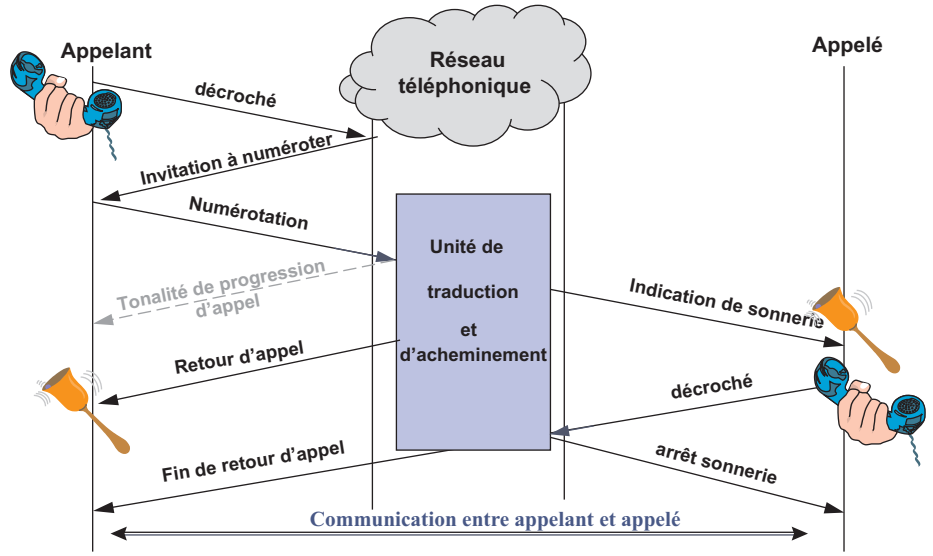


Figure 15.7 Diagramme d'une communication téléphonique.

La fin de communication est détectée par le raccroché (ouverture de la boucle de courant). Notons deux variantes lors de l'appel : la première correspond à l'incapacité du réseau à écouler la demande, l'appelant en est alors averti par un message du style : « Par suite d'encombrement... », la seconde correspond à l'occupation de la ligne appelée, l'appelant a alors, en retour, une tonalité spécifique dite tonalité d'occupation.

L'intention d'établir une communication est détectée par le décroché du terminal. Que se passe-t-il si on décroche le combiné mais que cette action n'est suivie d'aucune numérotation (décroché malencontreux) ? La détection du décroché monopolise des ressources dans le commutateur de rattachement (enregistreur). Pour libérer ces ressources, il est nécessaire d'inhiber le poste dont l'usage restera interdit jusqu'à ce que celui-ci soit raccroché.

La figure 15.8 décrit les différentes étapes du décroché malencontreux, la signification du diagramme est donnée ci-dessous :

2. Ce signal simulait le « bruit » généré par les commutateurs électromécaniques. Cette tonalité était destinée à faire patienter l'appelant pendant l'établissement du circuit. Avec les commutateurs électroniques de la dernière génération et l'utilisation d'une signalisation par canal sémaphore, la durée d'établissement du circuit est devenue très faible et ce signal n'avait plus de raison d'être.

– lorsque l'appelant décroche le combiné, le réseau (le commutateur de rattachement) détecte la fermeture de la boucle de courant ;
– il envoie à l'usager l'invitation à numéroter (signal à 440 Hz). Dans le même temps, il arme une temporisation ;
– le demandeur n'effectuant aucune opération, à l'échéance du compteur (Timer, de 15 à 20 secondes) le commutateur de rattachement inhibe le poste en lui envoyant la tonalité d'occupation (signal de décroché malencontreux) pendant environ une minute.

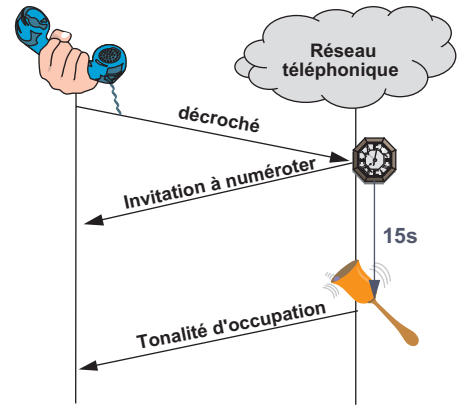


Figure 15.8 Diagramme des événements lors d'un décroché malencontreux.

15.3.4 La numérotation

Préfixe international	Indicatif Pays	Numéro national demandé		
		EZ	AB PQ	MC DU
Pour sortir du réseau national, en France 00	Par exemple France = 33	Exploitant Zone	Numéro du commutateur de rattachement	Numéro de la ligne d'abonné

Valeur E	Signification
0	Opérateur de boucle locale
1	Numéros d'urgence
2	Siris
3	Numéros spéciaux (téléservices)
4	Télétel 2
5	Omnicom
6	Esprit Telecom
7	Cegetel
8	France Télécom
9	9 Télécom

Figure 15.9 Structure d'un numéro d'abonné et valeur du préfixe E.

Le numéro d'abonné (Numéro international au format E.163 ou E.164) correspond à l'identification du point d'accès au réseau (prise terminale). L'adresse est du type hiérarchique, la structure en est donnée par la figure 15.9. Les différents éléments qui la constituent sont :

© Dunod – La photocopie non autorisée est un délit

– la désignation de l'exploitant (**E**), ce numéro n'a de valeur que sur le territoire français, il doit être omis pour un appel de l'étranger[3] ;
– la zone d'appel (**Z**), la France est divisée en 5 zones ;
– le commutateur de rattachement désigné par le sigle **ABPQ**[4] ;
– enfin, les 4 derniers chiffres (**MCDU**, Milliers, Centaines, Dizaines, Unités) qui désignent l'abonné local.

Il existe trois types de numérotation, La plus ancienne, la numérotation décimale ou analogique (33/66 ou 10 Hz) est réalisée par le cadran de la figure 15.5. Ce dernier provoque des ruptures de circuit. Les numéros sont envoyés au commutateur de rattachement sous forme d'impulsions de 66 ms suivi d'un repos de 33 ms, d'où le nom de système 33/66. Le 1 correspond à une rupture, le 2 à deux... le 0 à dix ruptures (figure 15.10).

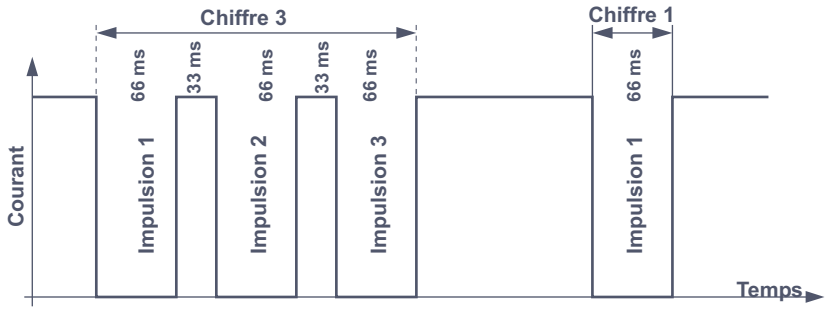


Figure 15.10 Exemple de numérotation décimale de 31.

Dans la numérotation fréquentielle ou vocale (multifréquentielle), normalisée par le CCITT (Q.23), l'enfoncement d'une touche génère deux signaux de fréquences différentes (une fréquence haute suivie d'une fréquence basse, **DTMF**, *Dual-Tone MultiFrequency*) transmis au central de rattachement. Chaque combinaison de fréquences a été déterminée pour minimiser le risque qu'une combinaison de voix lui ressemble. Les postes comportent 12 ou 16 touches, les touches A, B, C, et D peuvent être affectées à des fonctions particulières (figure 15.11). Certains postes téléphoniques fréquentiels ont la possibilité d'émettre une numérotation décimale.

Enfin, avec la dernière génération de postes téléphoniques spécifiques dits postes numériques, la numérotation correspond à la transmission d'une valeur binaire sur une voie dite de signalisation. La numérotation peut être propriétaire (poste numérique propriétaire) ou normalisée (poste RNIS).

15.3.5 Les modes de signalisation

Dès le décroché et jusqu'au raccroché, de nombreuses informations gèrent la communication téléphonique. Ces informations constituent la signalisation. Lors de l'établissement d'une

3. Le nombre d'opérateurs étant supérieur aux capacités de numérotation, l'ART (Autorité de Régulation des Télécommunications) a remis en vigueur l'utilisation du préfixe 16 suivi de deux chiffres. Exemple : 16 01 désigne Prosodie...

4. La signification d'ABPQ semble oubliée. Pour certains, ces chiffres désignaient les abonnés d'un même quartier reliés à un même central (ABPQ, ABonnés Par Quartier).

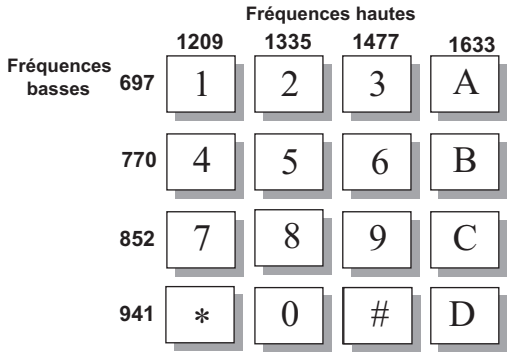


Figure 15.11 Clavier des postes à fréquences vocales.

communication, des informations de signalisation sont échangées entre l'usager et le réseau : le décroché, l'invitation à numéroter, la numérotation, le retour d'appel, le décroché du correspondant... , cette signalisation est dite signalisation Usager/Réseau. D'autres, nécessaires à l'établissement du circuit et à la supervision du réseau, n'intéressent que le réseau, c'est la signalisation réseau. Deux modes de transport des informations de signalisation sont utilisés en téléphonie (figure 15.12).

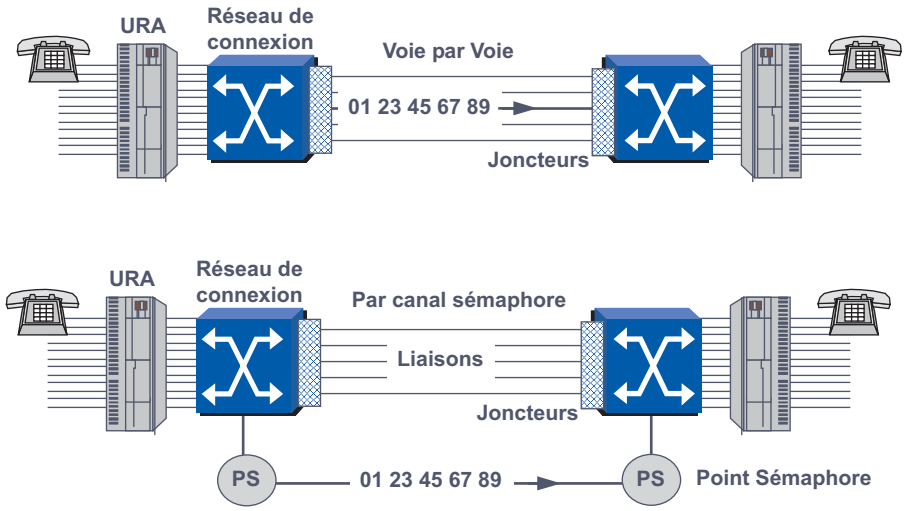


Figure 15.12 Les modes de signalisation.

Dans la signalisation **voie par voie** ou signalisation CAS (*Channel Associated Signalling*), une voie de communication correspond une voie de signalisation, la signalisation est associée à la communication. Ce qui nécessite l'établissement du circuit pour qu'elle soit transmise. Cette signalisation est dite en mode événement, c'est-à-dire qu'à un événement spécifique est associé un état électrique (impulsion...). La numérotation est transmise sur les fils de voix. La signalisation voie par voie peut être dans la bande (Amérique du Nord et Japon) ou hors bande. Elle a pratiquement disparu des réseaux publics mais subsiste sur la ligne de raccordement d'un usager analogique et dans de nombreuses installations téléphoniques privées

© Dunod – La photocopie non autorisée est un délit

La signalisation par **canal sémaphore** ou signalisation **CCS** (*Common Channel Signaling*) utilise un canal dédié (multiplexage avec les voies de communication) pour signaler tous les événements relatifs à un ensemble de circuits, la numérotation est acheminée sur le canal sémaphore en mode message. Les informations de signalisation sont transmises hors communication, ce qui autorise de nombreux téléservices. Le protocole de signalisation peut être normalisé ou propriétaire (protocole propre à un constructeur).

15.4 ÉVOLUTION DE LA TÉLÉPHONIE, LE RNIS

15.4.1 De l'accès analogique à l'accès numérique

La numérisation du réseau nécessite une conversion analogique/numérique en entrée du réseau et numérique/analogique en sortie. Un usager qui désire utiliser *n* communications téléphoniques simultanées doit être raccordé par *n* lignes (lignes groupées, les lignes groupées sont vues, pour le réseau, sous un même numéro). La numérisation autorise le multiplexage, d'où l'idée de réaliser des liaisons numériques de bout en bout, une seule ligne physique peut alors acheminer plusieurs communications téléphoniques (figure 15.13).

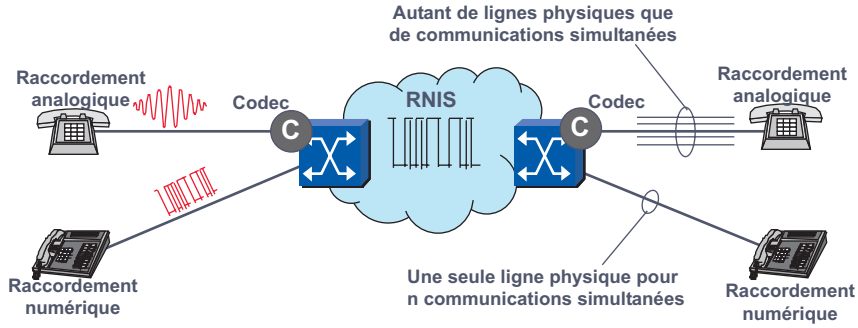


Figure 15.13 De l'analogique au numérique.

En réservant un IT (Intervalle de Temps) à la signalisation (débit de 64 kbit/s), on peut acheminer celle-ci en mode messages via un protocole de haut niveau. De ce fait, la signalisation peut être enrichie et autoriser de nombreux services nouveaux, c'est le **RNIS** (Réseau Numérique à Intégration de Service ou **ISDN**, *Integrated Service Digital Network*).

15.4.2 Le concept d'intégration de services

Le RNIS est une approche service du réseau devenu alors le réseau unique qui permet, à partir d'un seul raccordement, de disposer à la fois de services voix (téléphonie), vidéo (visiophonie, téléconférence[5]), de transmission de données en mode paquets ou autre et de la transmission de l'écrit (télécopie). La figure 15.14 schématise cette évolution, en RNIS, si un télécopieur initialise un appel, seul le télécopieur de l'installation destination « sonne ».

Le raccordement de terminaux différents (voix, données, images) sur une même ligne nécessite une signalisation spécifique et enrichie qui permette, à la fois, l'identification du terminal

5. La visiophonie est un service vidéo associé à téléphonie, les correspondants se voient durant la communication. La téléconférence consiste en l'organisation de conférences vidéo à partir d'un studio de télévision.

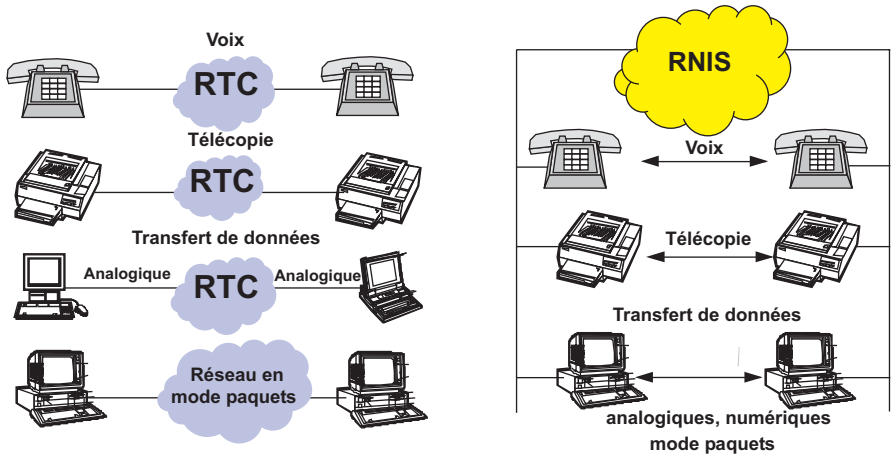


Figure 15.14 Évolution des accès avec le concept RNIS.

et le type de service requis. C'est ainsi, que le RNIS distingue les canaux de transmission (transport) de données ou canaux B établis appel par appel (circuits commutés), du canal de signalisation ou canal D établi de manière permanente et transportant les informations nécessaires à l'établissement du circuit (adresse, type de service invoqué...).

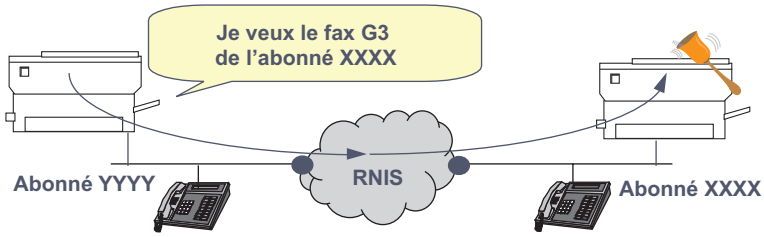


Figure 15.15 L'accès direct au service demandé.

Lors de l'émission d'un appel, celui-ci est pris en compte par le protocole de signalisation. La demande d'établissement de circuit est acheminée en dehors de toute communication établie. Elle transporte les informations en relation avec le numéro de l'appelé, le type de service invoqué... Ainsi, dans l'exemple de la figure 15.15, l'appel émis à partir du télécopieur de l'appelant invoquera un service de télécopie chez l'abonné distant. Seul alors un télécopieur répondra à cet appel. Le téléphone de l'installation a bien reçu l'appel, mais non concerné par le service invoqué ne sonne pas.

15.4.3 Structure du réseau

Un terminal RNIS utilise deux connexions : une connexion commutée à un canal B (*Bearer channel*) utilisé pour le transport d'informations utilisateur à 64 kbit/s (voix, données et images) et une connexion permanente sur le canal de signalisation (canal D, *Data channel*) de 16 ou 64 kbit/s. Des débits plus importants peuvent être obtenus par agrégation de plusieurs canaux B, on parle alors de canaux H (*High speed channel*) qui offrent un débit de 384 kbit/s

© Dunod – La photocopie non autorisée est un délit

(H_0), 1 536 kbit/s (H_{11}) ou de 1 920 kbit/s (H_{12}). La figure 15.16 illustre le principe de raccordement d'un terminal au réseau RNIS.

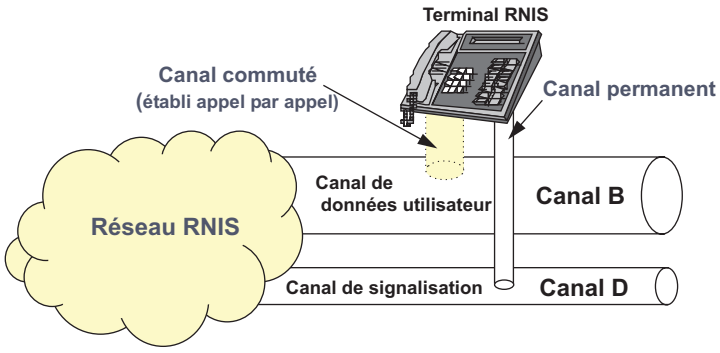


Figure 15.16 Connexions d'un terminal RNIS.

La connexion permanente du terminal au canal de signalisation rend obsolète la notion de terminal occupé : le terminal pourra toujours être alerté d'un appel entrant et recevoir, via le canal D, des messages (mini-messages). RNIS est donc un système de transmission utilisant deux réseaux distincts : un réseau de transmission (commutation de circuits) et un réseau de signalisation (commutation de paquets). Les réseaux sont fonctionnellement différents. Cependant, ils utilisent les mêmes capacités de transport (multiplexage) mais les commutateurs sont différents bien que situés sur les mêmes sites. La figure 15.17 illustre ce concept.

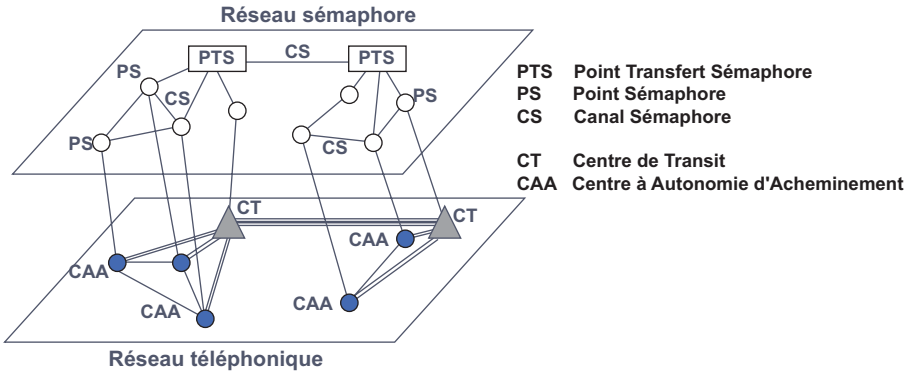


Figure 15.17 Réseau téléphonique et réseau sémaphore.

15.4.4 Le raccordement d'usager

Les accès RNIS

L'accès au réseau RNIS s'effectue par l'intermédiaire d'interfaces normalisées appelées points de référence (recommandation I 411 du CCITT) et dépendant du type de terminal à raccorder. Les terminaux n'accèdent pas directement au réseau, ils y sont raccordés via des interfaces. L'équipement d'interfaçage entre l'installation d'abonné et le réseau porte le nom de **TNR** (Terminaison Numérique de Réseau) ou de **TNL** (Terminaison Numérique de Ligne) selon le

type d'abonnement au réseau. La **TNA** (Terminaison Numérique d'Abonné) est un équipement facultatif, généralement un commutateur téléphonique privé (**PABX**, *Private Branched eXchange*). Lorsque l'installation d'abonné ne comporte pas de TNA, les points de référence S et T sont confondus.

Les divers points de référence (figure 15.18) sont, par ordre alphabétique, du privé vers le réseau public :

– **Point R**, interface pour les terminaux non RNIS, c'est notamment le cas des terminaux dotés d'une interface V.24/28, X.21, V.35...

– **Point S**, point d'accès universel pour les équipements compatibles RNIS,

– **Point T** matérialise la limite entre le réseau public et l'installation d'abonné, c'est aussi la frontière de responsabilité entre l'opérateur et l'abonné,

– **Point U**, il symbolise la limite entre le réseau de transport et la liaison d'abonné.

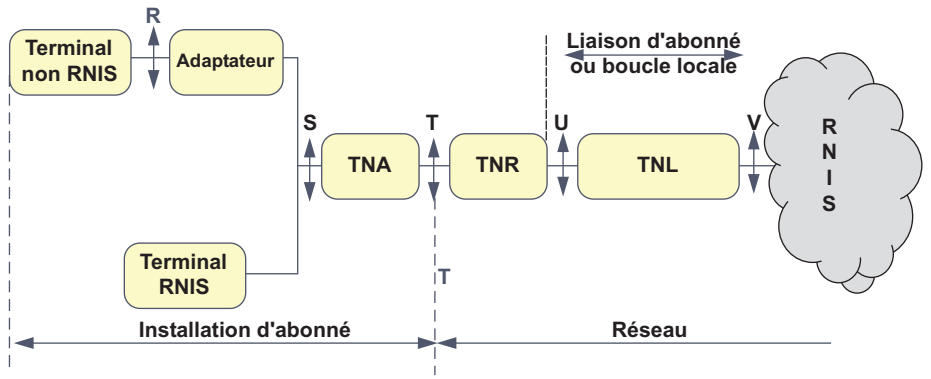


Figure 15.18 Les points de référence des accès au RNIS.

L'offre RNIS se décline selon la combinaison des trois types de canaux mis à disposition :

– les **canaux B** sont les canaux de transfert d'information, le débit nominal est de 64 kbit/s ;

– le **canal D**, à 16 ou 64 kbit/s selon le nombre de canaux B offerts, est dédié au transfert de la signalisation (protocole D). La bande non utilisée par la signalisation peut être utilisée pour transférer des données en mode paquet (accès aux réseaux X.25) ;

– les **canaux H**, combinaison de n canaux à 64 kbit/s offrent un débit de $n \cdot 64$ kbit/s. On distingue les canaux H_0 à 384 kbit/s, H_{11} à 1 536 kbit/s et H_{12} à 1 920 kbit/s. Les canaux B sont commutés et établis appel par appel sans garantie du chemin.

Selon le nombre de canaux offerts, on définit trois types d'accès, dont seuls deux sont disponibles en France :

– **T0**, ou accès de base (**BRI**, *Basic Rate Interface*), offre un débit de 192 kbit/s dont 144 utiles, soit 2 canaux B et un canal D à 16 kbit/s,

– **T1**, non disponible en France,

– **T2**, ou accès primaire (**PRI**, *Primary Rate Interface*) offre 15, 20, 25 ou 30 canaux B et un canal D à 64 kbit/s. Soit, pour 30 canaux B un débit de 2 048 kbit/s dont 1 920 utiles.

© Dunod – La photocopie non autorisée est un délit

Les accès peuvent être regroupés en « groupement d'accès » (plusieurs accès pour un même site, vus comme un seul faisceau). Le groupement d'accès de base est limité à six accès de base.

L'installation d'abonné

D'une manière générale, les terminaux RNIS sont reliés en bus. Selon l'équipement d'accès, l'installation est dite à bus passif si celle-ci est directement connectée à la TNR et à bus unique ou étoile de bus lorsque le (ou les bus) est (sont) raccordé(s) par l'intermédiaire d'un équipement local (TNA). La figure 15.19 représente ces différents modes de raccordement.

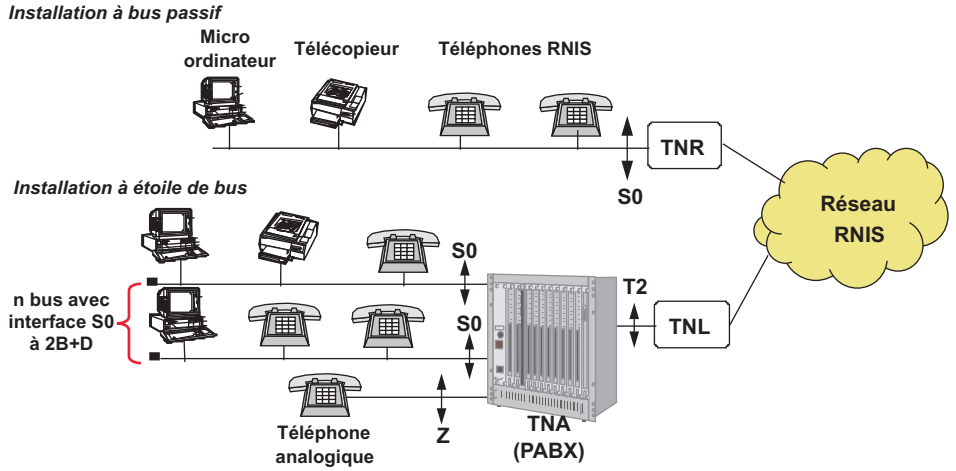


Figure 15.19 Structure des installations d'abonné.

15.4.5 Les services du RNIS

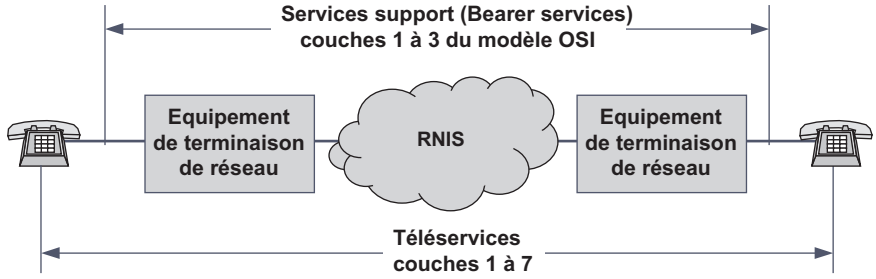


Figure 15.20 Modèle OSI et services RNIS.

Les réseaux RNIS donnent accès à trois types de services : les services supports pour le transfert d'information (couches 1 à 3 du modèle OSI), les téléservices qui sont des services complets (téléphonie, télécopie...) correspondant aux couches 1 à 7 du modèle OSI (figure 15.20), enfin des compléments de services qui étendent les possibilités du service transport ou des téléservices. Les compléments de services sont optionnels et facturés en sus de l'abonnement.

Le service support

Le service support est un service de transport d'information de bout en bout entre deux interfaces. Le RNIS offre trois types de service support : le service téléphonique, le service numérique sur canal B (transparent aux protocoles) et le mode paquets sur le canal D.

Le service téléphonique correspond aux services traditionnels existants sur le réseau téléphonique commuté, c'est-à-dire les services ne requérant qu'une bande analogique de 300-3 400 Hz. Dans ce type de service, dit de « qualité vocale », la continuité numérique n'est pas garantie de bout en bout, certaines artères empruntées peuvent être analogiques. C'est, par exemple, le cas d'un abonné RNIS appelant un abonné non RNIS (téléphonie à 3,1 kHz, télécopie groupe 3, modem audiofréquence, Minitel...). Ce service est désigné par le sigle **CCBNT** (Circuit Commuté B Non Transparent). Le service numérique garantit une qualité numérique de bout en bout. Il est utilisé pour les applications informatiques à faible ou moyen débit ($\leqslant$ 64 kbit/s), la télécopie groupe 4, la téléphonie 7 kHz, l'audio et la visioconférence. Ce service est désigné sous le nom de **CCBT** (Circuit Commuté B Transparent).

Les services CCBNT et CCBT sont offerts sur le canal B. C'est le terminal appelant qui effectue la demande de qualité de service en positionnant l'élément d'information « Mode de fonctionnement » du message d'établissement à 16 pour le service CCBT ou à 32 pour le service CCBNT. Un appel téléphonique est toujours établi en CCBNT.

Toute la bande passante du canal D n'est pas utilisée intégralement pour la signalisation. Ce lien étant établi de manière permanente, la bande disponible peut être utilisée pour réaliser un accès permanent[6], à 9 600 bit/s, aux réseaux en mode paquet X.25.

Les téléservices

Les téléservices sont des services de bout en bout entre deux terminaux couvrant l'intégralité des fonctions des couches 1 à 7. La signalisation assure la compatibilité entre les terminaux vis-à-vis des services invoqués. C'est ainsi, par exemple, qu'à un appel entrant provenant d'un télécopieur groupe 3, seul répondra un télécopieur groupe 3. Les téléservices normalisés sont : la téléphonie 3,1 kHz, la téléphonie 7 kHz, le vidéotex (Minitel), la télécopie groupe 3 et 4, la vidéoconférence... Ces services sont accessibles par un terminal RNIS (Interface S) ou un terminal analogique via un adaptateur audiofréquences.

Les compléments de service

Les compléments de service correspondent essentiellement à un enrichissement de l'offre téléphonique, ils concernent le service support et les téléservices. Ces prestations optionnelles donnent lieu à facturation (abonnement ou appel par appel).

➤ Coût total, Indication de coût

L'usager peut obtenir, en fin de communication, le coût total de la communication ou, durant la communication suivre l'évolution du coût de celle-ci (Indication de coût). Ces prestations ne fournissent que le coût global exprimé en unités téléphoniques (UT) de la communication au temps, sans tenir compte des compléments de service éventuellement invoqués.

6. Ce service a été étudié à la section 11.3.2.

© Dunod – La photocopie non autorisée est un délit

➤ Présentation d'appel, double appel, va-et-vient

Durant la communication, si un nouvel appel survient, l'usager en est averti (Présentation d'appel). Celui-ci peut achever la communication en cours et prendre la nouvelle, ou mettre la communication en cours en attente et prendre la nouvelle (Double appel). L'usager peut aussi passer alternativement de l'une à l'autre (Va-et-vient). L'usager ne peut prendre une troisième communication, celle-ci lui est cependant présentée.

➤ Identification d'appel, non-identification, identification d'appel malveillant

Un appel entrant est présenté avec l'identification de l'appelé (Identification d'appel) sauf si l'appelant a souscrit au complément de service « non-identification d'appel ». L'identification d'appel malveillant permet à un usager de faire identifier par l'opérateur l'auteur d'un appel malveillant.

➤ Portabilité

C'est la faculté dont dispose l'usager, durant un appel, de suspendre une communication et de reprendre celle-ci plus tard sur le même poste au même endroit ou sur le même poste déplacé dans l'installation ou encore sur un autre poste de la même installation. La suspension de l'appel n'interrompt pas la facturation. Elle est limitée à 3 minutes.

➤ Renvoi du terminal, transfert d'appel national

Un utilisateur peut faire réacheminer ses appels sur un autre poste de l'installation (Renvoi d'appel) ou sur un autre poste d'une autre installation (Transfert d'appel national). Le renvoi d'appel peut être inconditionnel, sur occupation ou sur non-réponse.

➤ Mini-message (Signalisation d'usager à usager)

Cette facilité permet aux usagers de s'échanger des messages de 32 caractères (Mini-message) en dehors de toute communication lors des phases d'établissement ou de libération de la communication.

➤ Services restreints

Ce complément de service permet de limiter l'usage d'un poste aux communications locales, de voisinage ou nationales.

➤ Sous-adresse

Cette information complète l'adresse du terminal, soit pour distinguer celui-ci, soit pour sélectionner sur celui-ci un service particulier (exemple : terminal multimédia). La sous-adresse peut contenir jusqu'à 40 caractères IA5. La sous-adresse est transportée de manière transparente sur le réseau.

➤ Sélection Directe à l'Arrivée (SDA)

La sélection directe à l'arrivée permet de joindre directement un terminal de l'installation sans nécessiter le recours à un(e) standardiste. C'est l'équipement local de l'abonné (PABX) qui effectue la relation entre le numéro SDA appelé et le numéro interne du poste demandé.

Généralement, ces deux numéros correspondent. Le numéro local attribué au poste correspond alors au MCDU du réseau public (quatre derniers chiffres du numéro public d'abonné).

Un numéro SDA est un service, le nombre de SDA d'une installation est indépendant du nombre de lignes de raccordement (canaux B) de l'installation. Les numéros SDA fournis peuvent être consécutifs ou disjoints. Soit, par exemple, pour une série de 100 numéros, les numéros M000 à M099 ou M000 à M0050 et M550 à M599 où M représente le chiffre des milliers.

15.4.6 Signalisation et le réseau RNIS

Généralités

Le RNIS utilise trois signalisations transportées dans deux protocoles (figure 15.21) :

– une signalisation usager/réseau ou protocole D ;

– une signalisation usager/usager pour les téléservices ;

– une signalisation interne au réseau transporté par un réseau de signalisation. Conforme à l'avis CCITT N°7, elle assure le transport de la signalisation protocole D (signalisation usager/réseau) et de la signalisation usager/usager.

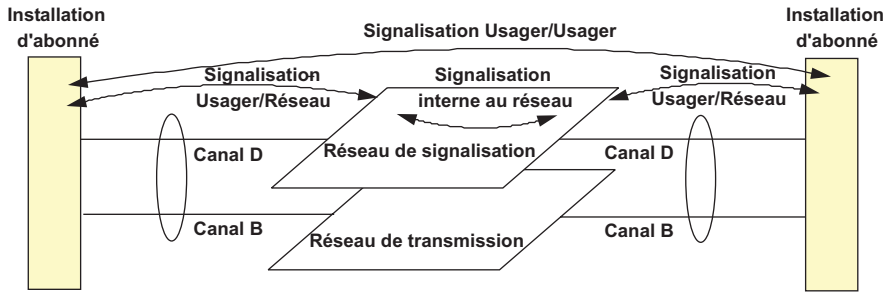


Figure 15.21 Signalisation et transmission dans un réseau RNIS.

La signalisation Usager

➤ Généralités

Les données de signalisation (niveau 3 du modèle OSI) entre le réseau et l'usager sont échangées en mode paquets. Le niveau 2 utilise une variante de HDLC, le protocole **LAP-D** (*Link Access Protocol on the D channel*). Les terminaux RNIS sont reliés en bus multipoint, il est donc nécessaire de les distinguer. L'adressage des terminaux (**TEI**, *Terminal End point Identifier*) et la désignation du service requis (**SAPI**, *Service Access Point Identifier*) se substituent au champ adresse d'HDLC (protocole en point à point). Hors ces différences, les fonctions de LAP-D sont conformes à celles d'HDLC.

La figure 15.22 montre l'encapsulation des données et l'organisation de la trame multiplexée pour un accès de base (2B+D), les différents champs seront expliqués par la suite. La trame multiplexée comporte en outre des bits d'écho du canal D (Bit E), des bits d'équilibrage de la composante continue (Bit L), des bits de synchro (Bit Q)...

© Dunod – La photocopie non autorisée est un délit

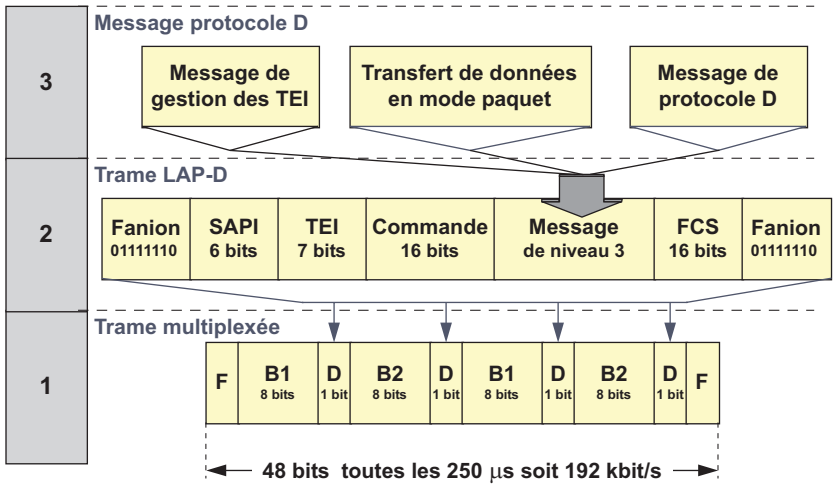


Figure 15.22 L'organisation générale de la trame multiplexée.

➤ Adressage des terminaux (TEI/SAPI)

Dans une configuration multipoint, les terminaux sont donc en compétition pour l'accès au canal D. De ce fait, à l'instar des réseaux locaux, il est nécessaire :

– d'identifier chaque terminal (adresse terminal) ;
– de définir le protocole de niveau supérieur ici, le service invoqué ;
– de résoudre les confits d'accès (collisions).

Le champ adresse de LAP-D se subdivise en deux sous-champs (figure 15.22) :

– le sous-champ **TEI** (*Terminal End-Point Identifier*) sur 7 bits identifie le terminal proprement dit. Cette adresse est similaire à l'adresse MAC des réseaux locaux. Les TEI peuvent être attribués par le constructeur (TEI de 0 à 63) ou par le réseau. La TNR (Terminaison Numérique de Réseau) attribue dynamiquement les TEI de 64 à 126. Le TEI 127 est réservé à la diffusion de messages. Lorsqu'un terminal à allocation automatique de TEI est connecté au bus, il demande au réseau de lui attribuer un TEI. Alors qu'un terminal à affectation non automatique s'assure de l'unicité de son TEI. Un terminal multifonction peut utiliser plusieurs TEI, un par fonction ;
– le sous-champ **SAPI** (*Service Access Point Identifier*) sur 6 bits indique le type de message transporté dans le champ information de la trame (identification du service requis). Les SAPI 32 à 47 sont réservés pour des usages nationaux, par exemple, en France le SAPI 32 est réservé au Télétex. La figure 15.23 présente les principaux SAPI utilisés.

➤ Les mécanismes d'accès au canal D et codage

Reliés en bus, les terminaux accèdent, au canal D, en compétition. Les conflits d'accès au canal D sont résolus par le protocole **CSMA**/CR (*Carrier Sense Multiple Access Contention Resolution*, accès multiple avec écoute de porteuse et résolution des collisions).

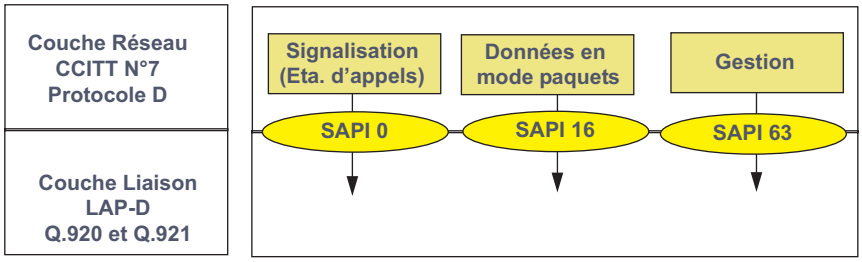


Figure 15.23 Affectation des principaux SAPI.

Le principe général de l'accès au canal D est similaire à celui utilisé dans les réseaux locaux de type « Ethernet ». Cependant, le support physique étant multiplexé, il peut y avoir une activité électrique sur celui-ci (canal B) alors que le canal D est libre. L'écoute doit se faire au niveau du canal et non du support. Pour détecter et prévenir une éventuelle collision toutes les données émises sur le canal D sont retransmises par la TNR sur un **canal d'écho** (**canal E**, figure 15.24). La station vérifie en permanence que ce qu'elle reçoit sur le canal E correspond bien à ce qu'elle a émis sur le canal D. Si ce n'est pas le cas la station s'arrête (collision). En l'absence d'émission, un terminal émet des « 1 » (potentiel électrique 0). Lorsqu'il désire accéder au canal D, le terminal écoute celui-ci, s'il ne détecte aucune activité durant un certain délai (8 à 11 temps bit selon le message à émettre), il émet sa trame LAP-D.

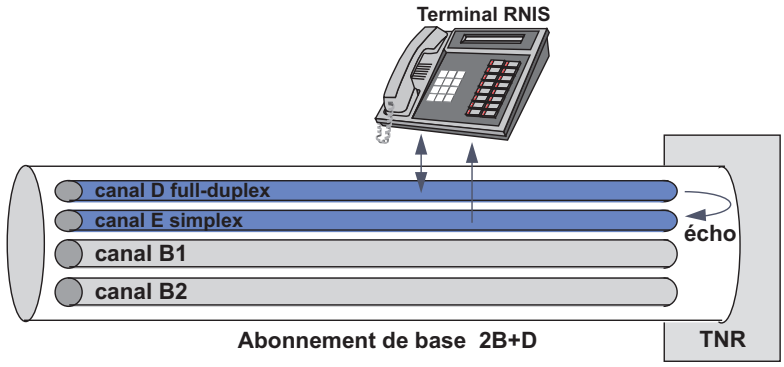


Figure 15.24 Le terminal émet sur le canal D écoute l'écho le canal E.

Afin d'éviter que toutes les stations en conflit ne s'arrêtent, un mécanisme de résolution de la contention (CSMA/CR) assure qu'une station, et une seule, pourra poursuivre son émission. Le système repose sur le codage retenu pour les signaux électriques, les zéros logiques correspondent à l'émission d'une tension alternativement positive ou négative (élimination de la composante continue), tandis que les 1 logiques correspondent à une tension nulle. Ce codage, appelé codage pseudo-ternaire, est représenté figure 15.25.

La répétition, par le canal E, des données du canal D est telle que, pour tout 1 émis, le canal E retransmet un 1 (tension nulle), pour tout 0 émis, le canal E retransmet un 0. C'est-à-dire que l'émission d'un 0 par une station masque l'émission d'un 1 par une autre. Ce mécanisme, illustré figue 15.25, autorise la résolution des conflits d'accès. Au temps d'horloge 1, 2, 3 et 4 les signaux émis sur le canal E correspondent à ceux émis par les divers terminaux, ceux-ci poursuivent leur émission.

© Dunod – La photocopie non autorisée est un délit

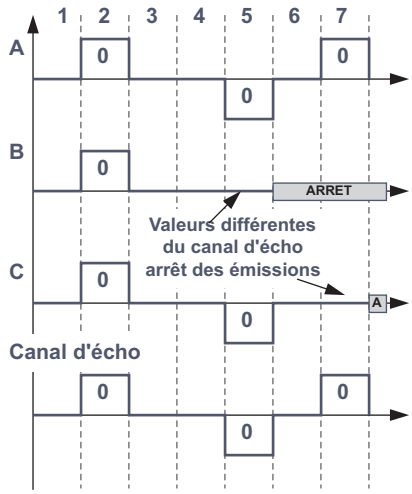


Figure 15.25 Mécanisme de résolution des contentions.

Au temps 5, le canal E retransmet le 0 des stations A et C, la station B qui avait émis un 1 cesse ses émissions. Au temps 7, c'est la station C qui a un écho différent, elle arrête ses émissions. Seule, la station A continue d'émettre. Ce mécanisme ne peut fonctionner que si toutes les stations émettent le premier 0 de la trame avec la même polarité, sinon deux 0 de polarité inverse s'annuleraient (niveau électrique nul). De ce fait, la règle d'alternance des 0 n'est pas respectée et la valeur continue peut ne plus être nulle, des bits d'équilibrage sont insérés dans la trame.

Trame LAP-D	Fanion	00 SAPI	1 TEI
TEI = 1	01111110	00 000000	1 0 0 0 0 0 1
TEI = 2	01111110	00 000000	1 0 0 0 0 1 **0**
TEI = 5	01111110	00 000000	1 0 0 0 1 **0** 1
Canal E			0 0 0 0 0 1

La station 5 s'arrête
La station 2 s'arrête

Figure 15.26 Priorité au terminal de plus faible adresse.

Le mécanisme adopté favorise les terminaux de plus faible adresse (figure 15.26). Pour compenser la priorité ainsi octroyée, une station qui a réussi à transmettre devra écouter le canal durant un temps bit de plus (9, au lieu de 8, pour les messages de signalisation et 11, au lieu de 10, pour les transmissions de données).

➤ Le niveau 2 : LAP-D (CCITT I.440/Q.920 et I.441/Q.921)

Le niveau 2 du RNIS est chargé d'assurer la transmission des trames entre un terminal et le réseau. Les fonctions assurées sont conformes au modèle de référence :

– ouverture et fermeture de session,

– détection et récupération des erreurs,

– numérotation des trames,

– contrôle de flux.

Hors l'adressage multipoint (adressage TEI/SAPI), le format de la trame LAP-D est similaire à celui du LAP-B (figure 15.27). Le protocole LAP-D utilise le format étendu (numérotation des trames modulo 128), la longueur maximale des trames est fixée à 260 octets.

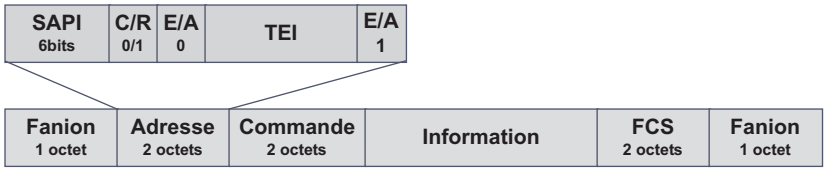


Figure 15.27 Format de la trame LAP-D.

Le champ adresse comporte les champs SAPI et TEI décrits plus haut. Le bit **E/A** (*End Address*, champ d'extension d'adresse) est à 0 dans le premier octet et à 1 dans le second (Fin du champ d'adresse). Enfin, le bit **C/R** (*Command/Respons*) distingue les trames de commande (C/R = 0) des trames de réponse (C/R = 1).

LAP-D utilise les trames UI (*Unnumbered Information*) pour échanger des messages hors connexion (messages d'établissement, messages de gestion des TEI...). Le format du champ d'information est illustré en figure 15.28.

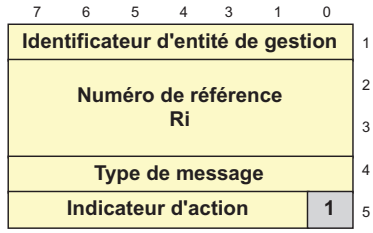


Figure 15.28 Format des messages des trames UI.

Gestion des TEI

Les procédures de gestion des TEI comprennent les procédures permettant : l'affectation, le contrôle et la suppression d'un TEI. Le format des messages de gestion des TEI a été fourni en figure 15.28, la signification et l'utilisation des différents champs sont indiquées dans la figure 15.29.

La figure 15.30 décrit un échange protocolaire d'affectation de TEI. Le terminal qui vient d'être raccordé au réseau lui demande de l'identifier (affectation d'un TEI, Type de message = 1). Le message est adressé à l'entité de gestion 63 (SAPI = 63), le champ Ai à 127 précise au réseau que toute valeur est acceptable par le terminal.

La référence d'appel (Ri) est un nombre aléatoire compris entre 0 et 65535, elle permet de distinguer d'éventuelles demandes simultanées. Le réseau peut affecter une valeur (Type de message = 2) ; dans ce cas, le champ Ai contient la valeur affectée (TEI = 64 à 126), il peut aussi refuser l'affectation (pas de TEI disponible) le type de message est alors 11 et le champ Ai contient 127.

© Dunod – La photocopie non autorisée est un délit

Messages	Identificateur d'identité	Référence Interne (Ri)	Type de Message	Indicateur d'action (Ai)
Demande d'identité U → R	0000 1111	0-65535	0000 0001	Ai = 127 Tout TEI est acceptable
Identité affectée R → U	0000 1111	0-65535	0000 0010	Ai = 64 à 126 Valeurs attribuées au terminal
Identité refusée R → U	0000 1111	0-65535	0000 0011	Ai = 64 à 126, valeurs refusées Ai = 127, pas de TEI disponible
Demande de contrôle d'identité R → U	0000 1111	Non utilisée mis à 0	0000 0100	Ai = 127, contrôler tous les TEI Ai = 0 à 126, valeur du TEI à contrôler
Réponse à contrôle d'identité U → R	0000 1111	0-65535	0000 0101	Ai = 0 à 126 Valeur du TEI déjà affectée
Suppression d'identité U → R	0000 1111	Non utilisée mis à 0	0000 0110	Ai = 127, suppression de tous les TEI attribués ; Ai = 0 à 126 TEI à supprimer

Figure 15.29 Codes des messages de gestion des TEI.

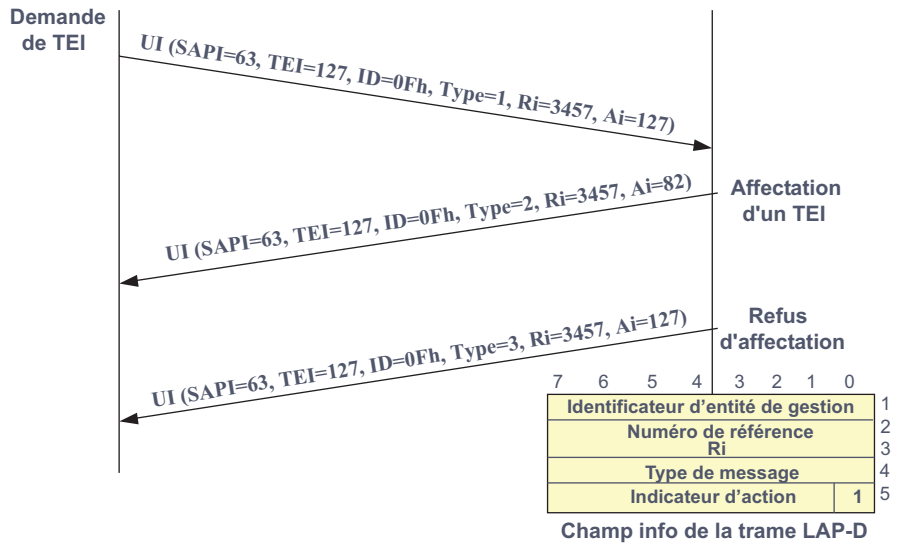


Figure 15.30 Affectation d'un TEI à un terminal.

➤ Le niveau 3 : le protocole D (CCITT I.450 et I.451)

Le protocole D gère les connexions (établissement, maintien et libération), il assure le transfert d'information usager/usager et la mise en œuvre des compléments de service. Le protocole D est véhiculé sur le canal D. La structure générale des messages est donnée par la figure 15.31.

7	6	5	4	3	2	1	0	
Discriminateur de protocole (Q.931/I.451)								1
0	0	0	0	1	0	0	0	
0	0	0	0	Longueur de la référence d'appel				2
F	Référence d'appel							3
0	Type de message							4
Éventuellement, autres éléments d'information								5

Figure 15.31 Structure du message.

Dans ce message, le premier octet est utilisé pour identifier le protocole Q.931 qui régit les échanges de messages usager/réseau. La référence d'appel identifie une connexion, elle n'a qu'une valeur locale (de manière similaire au NVL en X.25). Le bit F (fanion) permet de déterminer l'origine de l'appel (F = 0, message en provenance de l'origine d'appel ; F = 1, message en provenance du récepteur de l'appel). L'octet suivant identifie les différents types de messages.

Les différents types de messages sont :

– messages d'établissement d'appel (alerte, connexion, établissement...) ;
– messages d'information de l'appel (reprise, suspension...) ;
– messages de libération d'appel (déconnexion, libération, fin de libération) ;
– messages divers (information, facilité...).

L'étude détaillée de ces messages sort du cadre de cet ouvrage[7]. Cependant, citons par exemple, les éléments d'information d'un message d'établissement :

– mode de fonctionnement du support (parole, informations numériques...) ;
– identification de l'accès (accès de base, accès primaire, canal requis D ou B) ;
– compatibilité avec les couches supérieures (Normes CCITT ou CEPT) ;
– téléservice demandé (téléphonie, télécopie G3 ou G4, télétex, vidéotex, télex, application ISO...).

La figure 15.32 représente les échanges de messages pour un appel entrant ; les deux postes de l'installation y répondent, le poste qui décroche en premier obtient la communication. À la réception de l'appel entrant, le réseau émet une trame UI, c'est une trame d'information non numérotée permettant l'envoi du message d'établissement à tous les terminaux (TEI 127) en mode non connecté. Les terminaux 64 et 65 répondent, ils émettent vers le réseau une demande de connexion (**SABME**, *Set Asynchronous Balanced Mode Extended*, niveau trame) et déclenchent la sonnerie du poste. Le réseau accuse réception de cette demande de connexion (**UA**, *Unnumbered Acknowledgement*). La connexion étant établie, les terminaux adressent une alerte au réseau, l'appelant reçoit une indication d'appel (retour de sonnerie).

7. Pour illustrer le fonctionnement du protocole D, une analyse de trace du protocole D sera fournie en exercice.

© Dunod – La photocopie non autorisée est un délit

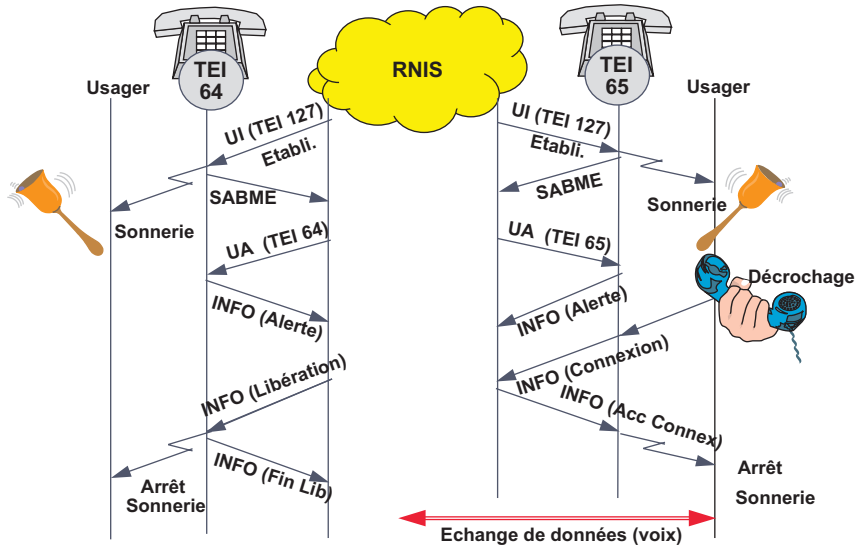


Figure 15.32 Diagramme des échanges lors d'un appel entrant.

Un utilisateur décroche le poste 65 (TEI 65), une demande de mise en relation est émise (Demande de connexion). Le réseau accepte cette demande (ACC_Connex) et libère (LIB) le poste 64 (TEI 64). Celui-ci arrête la sonnerie et accuse réception de la libération (FIN_LIB). L'échange d'information peut alors s'effectuer entre l'appelant et le poste 65.

La signalisation interne au réseau

➤ Objet

La signalisation interne au réseau par canal sémaphore ou système N°7 (**SS7**, *Signaling System 7*) définit les protocoles d'échange d'information de signalisation dans un réseau numérique entre :

– deux commutateurs pour l'établissement, l'administration et l'arrêt des communications ;

– un commutateur et une base de données pour la fourniture de services spécifiques (réseaux intelligents).

➤ Mode de fonctionnement

La signalisation sémaphore est du type hors bande. Cependant, selon le type de relation établi entre les points de signalisation, on distingue trois modes de fonctionnement (figure 15.33) :

– le **mode associé**, les commandes en relation avec les circuits entre deux commutateurs sont acheminées par un canal sémaphore reliant directement ces deux commutateurs ;

– le **mode non associé**, les commandes des circuits entre deux commutateurs transitent dans le réseau par des routes non prédéterminées ;

– le **mode quasi-associé**, les commandes des circuits transitent par des nœuds (PTS, Point de Transfert Sémaphore) prédéterminés (routage fixe).

Le réseau SS7, hors panne ou incident, utilise le mode quasi-associé qui garantit dans un réseau datagramme le séquencement des informations.

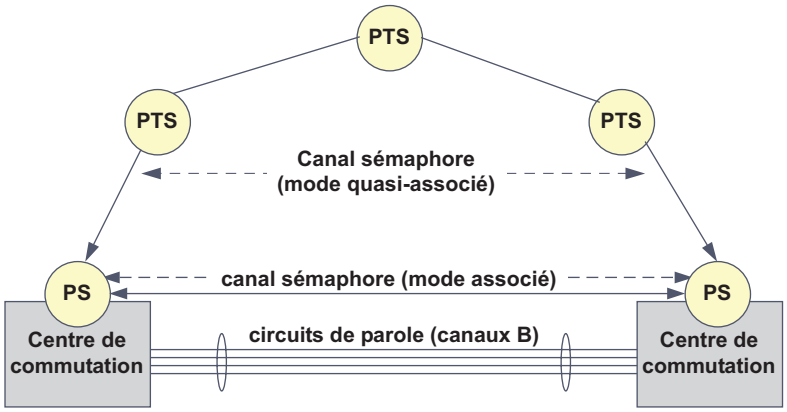


Figure 15.33 Les modes de fonctionnement d'un canal sémaphore.

➤ Architecture du système

La signalisation utilise une infrastructure de communication redondante qui forme le réseau de signalisation (figure 15.17). L'architecture du système de signalisation comporte deux sous-ensembles (figure 15.34).

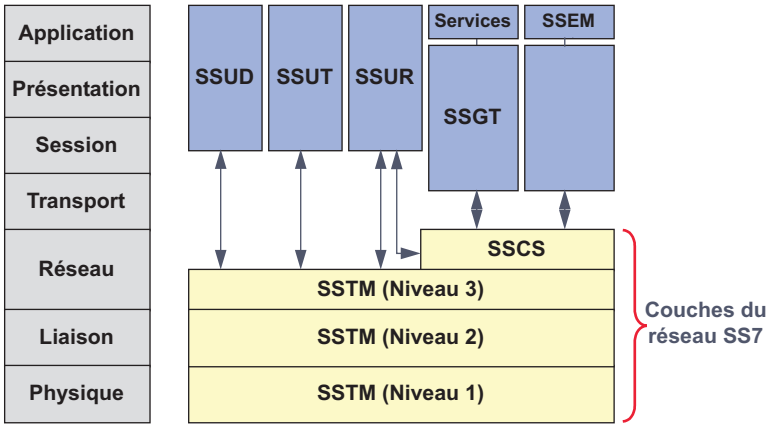


Figure 15.34 Architecture du système 7.

Le sous-système de transfert de message (**SSTM**) ou **MTP** (*Message Transfer Part*) correspond aux couches 1 à 3 du modèle OSI. Le niveau 1 (SSTM1) définit le transport de l'information dans un canal à 64 kbit/s (IT16 d'un multiplex primaire à 2,048 Mbit/s). Le niveau 2 (SSTM2) assure le transfert fiable des messages entre équipements du réseau. Le protocole, semblable à HDLC, permet la détection et la reprise sur erreur des trames ainsi que le contrôle de flux. La figure 15.34 fournit le format de la trame. Le niveau 3 (SSTM3) assure l'acheminement des messages dans le réseau (routage, réseau en mode datagrammes). Chaque **PS** (Point de Signalisation) est identifié par un code (*Point Code* sur 14 bits), le routage est du type fixe

© Dunod – La photocopie non autorisée est un délit

ce qui garantit le séquencement hors panne du réseau. La structure des messages de niveau 3 est donnée en figure 15.35.

Les sous-systèmes utilisateurs (**SSU**) ou **UP** (*User Part*) comportent :

– le sous-système utilisateur de données (**SSUD**) utilisé pour la signalisation dans les réseaux à commutation de données en mode circuits. Ce sous-sytème n'est pas utilisé dans le RNIS ;

– le sous-système utilisateur téléphonique (**SSUT**) assure la signalisation des communications téléphoniques ;

– le sous-système utilisateur RNIS (**SSUR**) définit les procédures de commande d'appel dans le RNIS ;

– le sous-système de commande de connexion de signalisation (**SSCS**) permet l'échange de message de signalisation hors mode circuits. Ce système constitue une interface entre le système de transport et le système de gestion et administration ;

– le sous-système de gestion des transactions (**SSGT**) permet d'assurer la mise en œuvre de compléments de service, de mécanisme de sécurité comme la gestion de groupes fermés d'usagers (GFU) ;

– le sous-sytème exploitation maintenance (**SSEM**) comporte les procédures de surveillance du réseau.

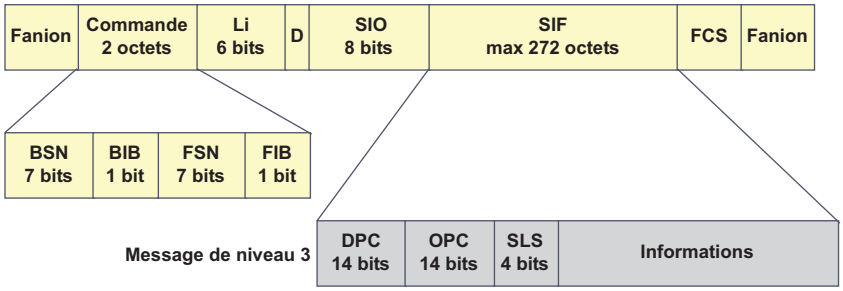


Figure 15.35 Format général des messages SS7.

La figure 15.35 représente la structure d'un message SS7. Le format général de la trame est similaire à celui d'HDLC (Fanion, Commande, FCS, transparence binaire). Le champ commande comporte les informations nécessaires au contrôle de séquencement et à la reprise sur erreur :

– **BSN** (*Backward Sequence Number*, numéro de séquence arrière) indique le numéro de séquence de la trame acquittée. Ce numéro correspond au Nr d'HDLC ;

– **BIB** (*Backward Indicator Bit*), à 1, ce bit correspond à un acquittement négatif et à une demande de retransmission de la trame BSN ;

– **FSN** (*Forward Sequence Number*, numéro de séquence avant) indique le numéro du message transmis. Ce numéro correspond au Ns d'HDLC ;

– **FIB** (*Forward Indicator Bit*), à 1 il indique que la trame FSN est une retransmission ;

– **LI** (*Length Indicator*) sur 6 bits indique en puissance de 2 la longueur du champ d'information décomptée par groupe de 8 octets ($L = 8 . 2^{LI}$) ;

– Disponible (2 bits) ;
– **SIO** (*Service Indicator Octet*) identifie le sous-système utilisateur requis, correspond à la notion de SAP (Service Access Point) ;
– **SIF** (*Signalling Information Field*) champ d'informations de signalisation limitée à 272 octets ;
– **DPC** (*Destination Point Code*) identifie le point sémaphore destination (adresse) ;
– **OPC** (*Originating Point Code*) identifie le point sémaphore source ;
– **SLS** (*Signalling Link Selection*) indication supplémentaire pour assurer un partage de charge dans le réseau. Le routage se fait en prenant en considération les trois champs (DPC, OPC, SLS).

Le champ d'information comprend notamment l'identification de l'appelé et de l'appelant, les informations de taxation (catégorie du demandeur) et, selon le message, une série d'indicateurs.

Évolution du RNIS

Ouvert en 1987 dans les Côtes d'Armor et disponible sur tout le territoire depuis 1990, le RNIS n'a pas eu à ses débuts, en raison du coût de l'abonnement et de communications plus chères, un franc succès. Il n'a connu un réel développement que lorsque France Télécom a retiré de son offre commerciale professionnelle les raccordements MIC. Aujourd'hui, la tarification des communications est unique quels que soient l'opérateur et le type de raccordement (RNIS ou analogique).

Développé dans le concept du réseau unique pour tous les services, le RNIS devrait évoluer vers des débits plus élevés. Le RNIS large bande (**B-ISDN**, *Broadband-ISDN*) s'appuyant sur la commutation de cellules (ATM) devraient offrir des débits allant de 155 à 622 Mbit/s et des téléservices du type vidéo haute définition pourraient alors être disponibles. Cependant, Internet et son protocole TCP/IP semble mieux placé aujourd'hui pour concrétiser le réseau multimédia du futur.

15.5 LA TÉLÉPHONIE ET LA MOBILITÉ

15.5.1 Principes généraux

Le besoin d'alerter ou de communiquer avec une personne en déplacement a conduit aux concepts de messagerie unilatérale (alerte à personne ou *paging*) et de radiotéléphonie cellulaire.

Le *paging* consiste à envoyer par diffusion à un petit terminal de poche un bip sonore ou un petit message alphanumérique. La communication est unilatérale, le message est transmis par Minitel ou par l'intermédiaire d'une opératrice. De ce fait, les techniques mises en œuvre pour le *paging* sont simples.

Il n'en est pas de même de la téléphonie mobile qui, en plein essor, soulève de nombreuses questions notamment :

– la bidirectionnalité de la communication et le nombre de communications à établir en même

© Dunod – La photocopie non autorisée est un délit

temps posent un problème d'allocation de fréquences. Le partage du spectre a introduit la notion de communication cellulaire. Une cellule est une zone dans laquelle les fréquences utilisées appartiennent à un même ensemble. Deux cellules adjacentes ne devront pas utiliser le même ensemble de fréquences ;

– l'accès multiple et le partage du support (politique d'accès) ;
– la localisation du mobile en déplacement ou itinérance (*roaming*) ;
– la possibilité pour le mobile en déplacement de maintenir la communication en cours (*hand over* ou *handoff*) ;
– la confidentialité des communications.

Structure générale d'un système de radiotéléphonie

La figure 15.36 décrit les différents composants d'un réseau de radiocommunication cellulaire de type **GSM** (*Global System for Mobile*, initialement Groupe Spécial Mobile).

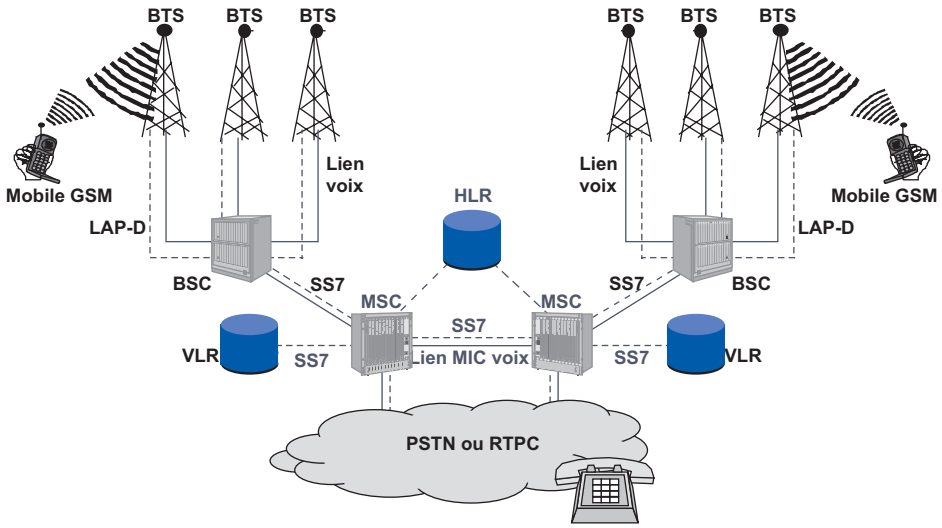


Figure 15.36 Principe d'un réseau GSM.

Un réseau de téléphonie mobile de type GSM comprend :

– des stations mobiles (**MS**, *Mobile Station* ou **mobile GSM**), celles-ci doivent être identifiées et localisées par le système pour pouvoir établir une communication (appel sortant) et être alertées (appel entrant) ;
– un sous-système radio (**BSS**, *Base Station Subsystem*) comportant un ensemble de bases radios (**BTS**, *Base Transceiver Station*) ou interfaces air qui gèrent le trafic radio avec le mobile. La zone couverte par une base radio (BTS) constitue une cellule. Une station de contrôle gère un ensemble de BTS (**BSC**, *Base Station Controller*) ;
– un sous-système réseau (**NSS**, *Network SubSystem*) comprenant les commutateurs de cœur de réseau (**MSC**, *Mobile services Switching Center*) associés à une base de données locale (**VLR**, *Visitor Location Register*) et une base de données centrale ou registre des abonnés nominaux (**HLR**, *Home Location Register*).

Principe général de fonctionnement

Chaque BTS diffuse en permanence sur un canal de signalisation (**BCCH**, *Broadcast Control CHannel*) des informations générales sur le type de réseau auquel la cellule est rattachée. Lorsqu'un mobile est mis sous tension, il recherche (*scanning*) un canal BCCH. Le mobile sélectionne alors la BTS (cellule) dont le niveau de réception est le plus élevé en acquittant le signal de BCCH sur le canal d'accès aléatoire de la cellule (**RACH**, *Random Access CHannel*) et s'y inscrit. Le réseau lui attribue alors un canal de signalisation (**SACCH**, *Slow Associated Control CHannel*). Les données utilisateurs de la HLR (base de données centrale) sont recopiées dans la VLR (base de données locale des visiteurs de la cellule). À la demande de la BSC, la HLR enregistre la localisation du mobile pour être en mesure d'y acheminer les appels entrants. En principe, la base HLR est unique par réseau (**PLMN**, *Public Land Mobile Network*).

15.5.2 Gestion de l'abonné et du terminal

On distingue plusieurs types de terminaux selon leur taille (terminaux portables et portatifs), leur bande de fréquences (GSM 900 MHz, DCS 1 800 MHz et les terminaux bi-bandes). L'utilisation de systèmes portables miniaturisés, facilement « empruntables » et d'une interface air a nécessité l'introduction de mécanismes d'identification garantissant une certaine sécurité et préservant l'anonymat des communications. C'est ainsi, que les identifications de l'abonné et du terminal ont été dissociées.

L'abonné est identifié par un module spécifique dans lequel sont inscrites toutes les données propres à l'utilisateur (carte **SIM**, *Subscriber Identity Module*). Cette carte, délivrée par l'opérateur, mémorise un nombre important d'informations :

– des données propres à l'opérateur (réseau...) ;
– des données propres à l'utilisateur (identification, services optionnels, annuaire...) ;
– des données propres à l'usage du terminal (dernière zone de localisation, listes des réseaux utilisés...) ;
– les informations de sécurité (mots de passe utilisateur, compteurs d'erreur, clé de déblocage, clé d'authentification, clé de cryptage propre au terminal...) ;
– les mini-messages reçus (**SMS**, *Short Message Service*)...

L'utilisation du portable est protégée par un mot de passe utilisateur demandé à l'initialisation du système (CHV1, *Card Holder Verification* ou code **PIN**, *Personnal Identity Number*), certaines fonctions ne sont accessibles qu'après l'introduction d'un mot de passe de second niveau (CHV2 ou PIN2).

La carte SIM permet de dissocier les données utilisateurs de celles du terminal et permettre à l'opérateur de bloquer l'un indépendamment de l'autre. Le terminal est identifié par **l'IMEI** (*International Mobile Equipement Identity*). À chaque utilisateur est associé un numéro d'appel international (**MSISDN**, *Mobile Station ISDN*) par lequel l'abonné peut être appelé et un identifiant utilisé par le réseau pour le localiser (**IMSI**, *International Mobile Subscriber Identity*). Lorsqu'un utilisateur est présent dans une zone, pour ne pas transporter dans le réseau son identifiant personnel (confidentialité), un identifiant temporaire lui est attribué (**TMSI**, *Tempo-*

© Dunod – La photocopie non autorisée est un délit

rary Mobile Station Identity). La figure 15.37 illustre l'utilisation de ces identifiants lors d'un appel entrant depuis le réseau public commuté (RTC).

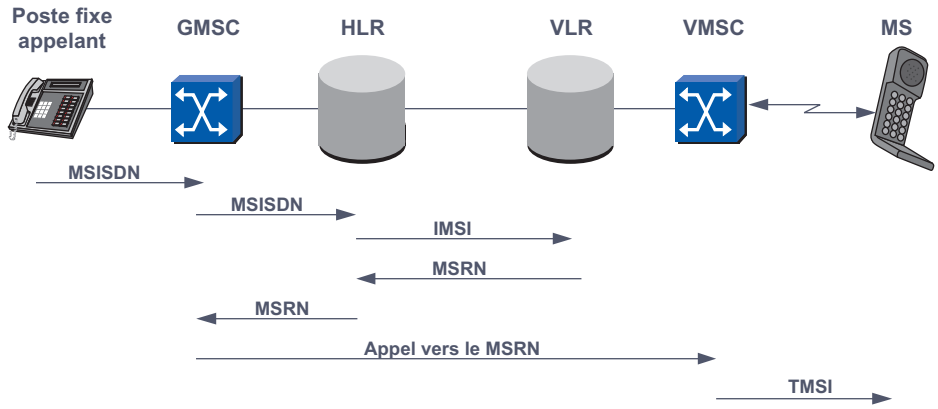


Figure 15.37 Echange des différents identifiants.

Le poste appelant numérote le MSISDN (06 xx xx xx xx), cet appel est acheminé par le réseau téléphonique fixe vers le commutateur du réseau de mobile le plus proche (MSC) qui fera office de passerelle entre les deux réseaux (**GMSC**, *Gateway MSC*). Le GMSC interroge le HLR pour connaître la localisation de l'appelé. Le HLR substitue au MSISDN le IMSI (N° attribué pour localiser l'appelé) et interroge la base VLR qui lui attribue alors un **MSRN** (*Mobile Station Roaming Number*), Numéro permettant le routage des appels, ce numéro est composé du code pays du VLR, de l'identifiant du VLR et du N° d'abonné). Le GMSC établit alors l'appel vers le **VMSC** (*Visited MSC*). Enfin, le VMSC établit l'appel vers le mobile en utilisant l'identité temporaire (TMSI).

L'affectation des canaux de communication est dynamique. Elle suit les procédures décrites ci-après. Lors d'un appel entrant, la base radio diffuse sur un canal d'appel (*paging*) l'identification de la station appelée. Le mobile qui reconnaît son identification accuse réception du message sur le canal de retour d'appel. La base radio affecte alors au mobile un canal de trafic (fréquence et IT). Lors d'un appel sortant, le canal de trafic n'est attribué par la base radio qu'après que l'appelant ait décroché. Cette technique dite du rappel du demandeur évite d'affecter des ressources à un appel non abouti.

15.5.3 L'interface radio

Organisation cellulaire du réseau

On appelle cellule, la zone géographique couverte par un émetteur (figure 15.38). La taille des cellules doit tenir compte de nombreux facteurs, notamment :

– des conditions de propagation. Les systèmes de téléphonie mobile utilisent des fréquences de l'ordre du GHz, la propagation de telles fréquences se fait uniquement par onde directe. Les obstacles créent des zones d'ombre ;

– de la limitation de la puissance d'émission du mobile. Un des éléments essentiels de la téléphonie mobile est le poids du terminal, ce facteur impose des batteries de faible capacité et donc, afin de disposer d'une autonomie suffisante, une puissance d'émission limitée ;

– du nombre potentiel de stations à accueillir vis-à-vis de la capacité d'accueil de la base radio. La bande de fréquence utilisée par les bases radio limite le nombre de canaux gérés par la station. Dans les zones à fort potentiel d'utilisateurs il sera nécessaire de réduire la taille des cellules pour accueillir convenablement tous les mobiles de la zone. De ce fait, les cellules seront plus petites en zone urbaine qu'en zone rurale ;
– de la vitesse de déplacement du mobile. La gestion du *hand over* est délicate, plus les zones sont petites vis-à-vis de la vitesse de déplacement du mobile plus le changement de cellules sera fréquent.

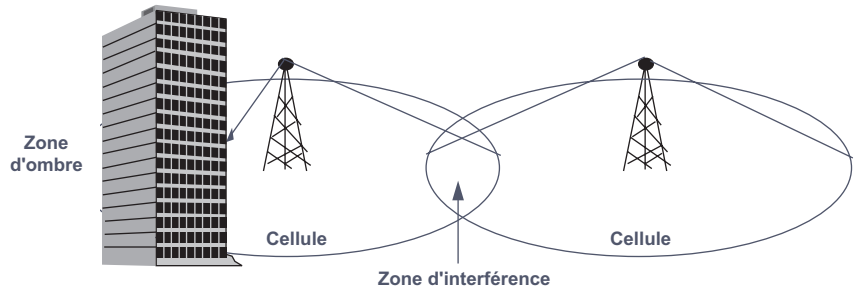


Figure 15.38 Couverture d'une liaison radio.

La limitation du spectre radio et les capacités d'un émetteur à gérer un nombre élevé de canaux radio conduisent à étudier la réutilisabilité des fréquences (bandes allouées). Les schémas de réutilisation des fréquences doivent tenir compte à la fois des puissances d'émission et des interférences (deux zones utilisant les mêmes fréquences ne doivent pas se perturber). Différents schémas de réutilisation sont utilisés, la figure 15.39 illustre un système à 9 fréquences (facteur de réutilisation 1/9). Les installations sans fil (*cordless*) privées (résidentielles ou derrière un petit PABX) peuvent être mono-cellulaire.

Figure 15.39 Organisation des cellules utilisant 9 jeux de fréquence de base.

L'accès partagé au support

L'accès de multiples mobiles à une seule base radio (BTR) conduit à définir une technique d'accès au support partagé. Ces techniques relèvent du multiplexage, la téléphonie mobile utilise :

– **l'AMRF** (Accès Multiple à Répartition de Fréquence, ou multiplexage fréquentiel ou **FDMA**, *Frequency Division Multiple Access*), une fréquence est allouée à chaque

© Dunod – La photocopie non autorisée est un délit

utilisateur. Ce système simple est cependant sensible au *fading* (combinaison d'ondes directes et réfléchies qui module la réception – effet d'évanouissement –) ;

– **l'AMRT** (Accès Multiple à Répartition dans le Temps, ou multiplexage temporel ou **TDMA**, *Time Division Multiple Access*), un intervalle de temps (IT) est alloué à chaque station. Plus souple que la précédente, cette méthode nécessite des systèmes de synchronisation ;
– la combinaison des deux dernières techniques **F/TDMA**, plusieurs canaux avec chacun un IT par utilisateur. Cette technique permet de multiplier les capacités d'accueil d'une base, elle est utilisée dans le système **GSM** ;
– **l'AMRC** (Accès Multiple à Répartition de Code ou **CDMA**, *Code Division Multiple Access*), une seule fréquence est utilisée et un code est attribué à chaque utilisateur. Cette technique est complexe mais accroît la capacité d'accueil des bases en simplifiant la gestion des fréquences.

Ces techniques ne permettent pas seulement l'accès simultané de plusieurs mobiles, mais aussi la gestion des différents trafics d'une même station (flux voix montant et descendant, signalisation...). Ces trafics sont répartis sur plusieurs canaux qui peuvent être en pleine bande ou à demi-bande par exemple :

– la voix peut être à pleine bande (compression 13 kbit/s) ou à demi-bande (6,5 kbit/s) ;
– les canaux de données peuvent à pleine bande offrir un débit de 9,6 kbit/s et à bande réduite seulement 4,8 kbit/s.

Gestion de la mobilité

La localisation (itinérance ou *roaming*) permet au réseau de transmettre un appel (appel entrant) alors que l'appelant n'a aucune connaissance de la position géographique de l'appelé. Le principe en est simple, lors de la mise sous tension le mobile s'identifie. Le MSC, centre de gestion local, de la cellule d'accueil interroge alors la base de données centrale (HLR) pour obtenir les informations relatives au visiteur et les inscrit dans la base de données locale (VLR). Le MSC attribue alors un identifiant temporaire au visiteur et informe la HLR de la position de celui-ci.

En permanence la base radio (BTS) analyse la qualité du signal reçu (canal de trafic ou voie de signalisation). En fonction de la qualité du signal, la station décide de maintenir le lien ou d'effectuer le transfert vers une cellule voisine. Le centre de gestion local demande alors aux cellules voisines d'effectuer une mesure de champ sur le canal d'émission du mobile. En fonction des résultats obtenus le centre de gestion détermine la cellule qui doit accueillir le mobile et donne l'ordre de transfert.

Le transfert intercellulaire est effectué sans interruption perceptible de la communication. Cependant, le temps de basculement n'est pas nul et reste un handicap au transfert de données. Le transfert de données à partir d'une station mobile n'est fiable que lorsque le mobile est fixe !

De même, l'analyse de la puissance reçue par la BTS, du rapport signal à bruit et du taux d'erreur peut conduire la BTS à demander au mobile une éventuelle réduction de puissance d'émission afin d'une part de ne pas perturber les cellules voisines et, d'autre part d'économiser ses batteries.

15.5.4 Description succincte des différents systèmes en service

Plusieurs produits de téléphonie mobile sont disponibles. Certains à usage résidentiel (Norme **CT1**, *Cordless Telephon 1 Generation*) sont d'un emploi courant et rien ne les distingue d'un combiné classique si ce n'est la mobilité dans la limite de portée de l'appareil. Ces postes utilisent généralement un système d'identification locale et de scanner pour éviter le piratage de la ligne, la borne fixe ne permet d'écouler qu'une seule communication. La bande de fréquence autorisée en France correspond à la fréquence intermédiaire des récepteurs de télévision, ce qui provoque parfois des intermodulations.

Le **GSM** (*Global Service for Mobile communication*) constitue en France l'offre numérique dominante (Orange, SFR). L'intérêt essentiel de cette offre est la confidentialité absolue des communications, l'identification de l'abonné par une carte à puce évite un usage frauduleux du poste mobile. Devant le développement important de la téléphonie mobile, les opérateurs doublent le réseau en utilisant la norme **DCS1800** (*Digital Cellular System* dans la bande des 1 800 MHz). Celle-ci constitue l'offre unique de Bouygues Télécom.

La figure 15.40 décrit succinctement les différentes normes et offres de services en France.

	CT0/CT1	Cellulaire analogique	CT2	GSM	PCN DCS1800	DECT
Usage	Domestique PBX sans fil	Mobile	Mobile piéton PBX sans fil	Mobile	Mobile	PBX sans fil
Technologie	Analogique	Analogique	Numérique	Numérique	Numérique	Numérique
Bande de fréquences en MHz	16/47 26/41 9 000	200 400 900	900	900	1 800	1 900
Mode d'accès	FDMA	FDMA	FDMA	TDMA		TDMA
Nombre de canaux par balise	8/15/40	24	40	72	144	144
Portée émetteur	200 à 300 m	35 km	200 à 300 m	35 km	7 km	200 à 300 m
Transmission données	Non	Limitée	Non	Oui	Oui	Oui
Confidentialité	Non	Non	Oui	Oui	Oui	Oui
Roaming	Non	Oui	Manuel	Oui	Oui	Manuel
Hand Over	Non	Oui	Non	Oui	Oui	Oui
Appel Entrant	Oui	Oui	Manuel	Oui	Oui	Manuel
Appel Sortant	Oui	Oui	Oui	Oui	Oui	Oui
Commercialisation	Grand public	Radiocom 2000 SFR Services arrêtés	Bi-Bop Service arrêté	Orange SFR	Orange SFR Bouygues Télécom	PABX Alcatel Matra...

Figure 15.40 Tableau comparatif des différents systèmes.

15.5.5 Le service transport de données sur la téléphonie mobile

La donnée en mode circuit sur le réseau GSM

Le service de données (fax, accès distant à un réseau, accès à Internet -WAP-) en mode circuits est disponible sur tout le réseau GSM. Les services accessibles dépendent du terminal GSM et

© Dunod – La photocopie non autorisée est un délit

de l'abonnement. Compte tenu des faibles possibilités des premiers récepteurs GSM, ceux-ci étaient plutôt utilisés comme interface mobile d'accès à un réseau (figure 15.41). Le canal voix étant optimisé pour le transfert de la voix, le débit maximal offert ne dépasse pas 14,4 kbit/s. Un système d'agrégation de canaux est envisageable (4 au maximum). Les communications sont facturées au tarif voix.

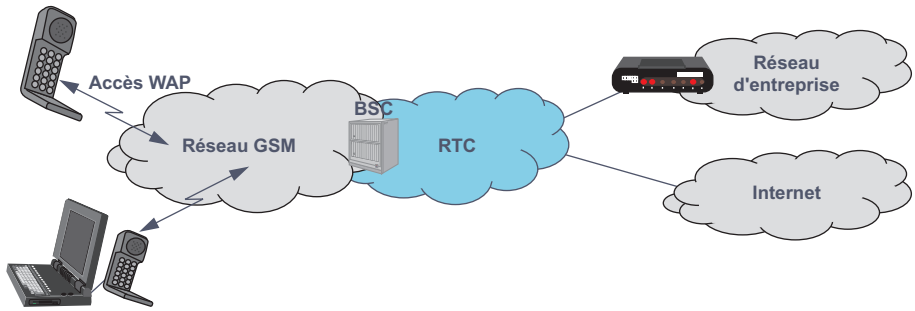


Figure 15.41 Accès au service données sur un réseau GSM.

La donnée en mode paquets sur le réseau GPRS

Le **GPRS** (*General Packet Radio Service*) est un réseau IP utilisant l'accès radio du réseau GSM. La figure 15.42 représente la structure d'un réseau GPRS.

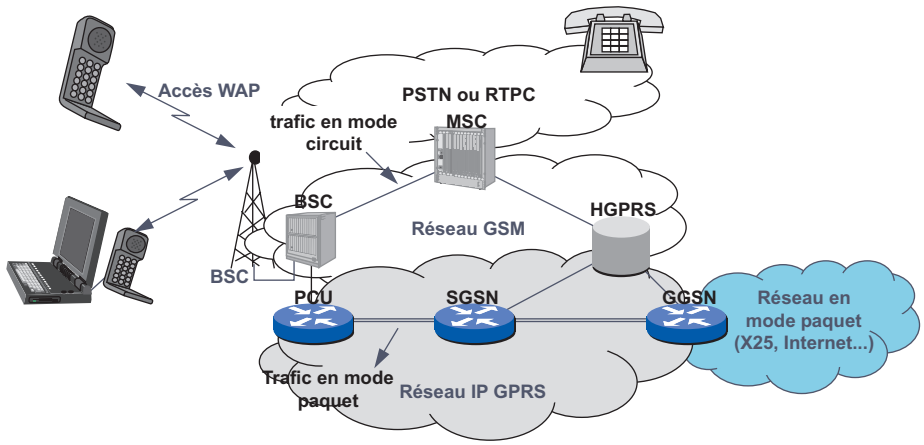


Figure 15.42 Structure d'un réseau GPRS.

Le réseau GPRS n'implique qu'une mise à jour du logiciel des éléments de base du réseau GSM (BTS et BSC) et l'introduction de nouveaux équipements dédiés réseaux mode paquets pour l'accès aux réseaux de données. Ces équipements sont :

– le **PCU** (*Packet Controler Unit*), implanté au niveau des contrôleurs de stations (BSC), assure l'adaptation des unités de données issues du mobile au format paquets et inversement ;

– le **SGSM** (*Serving GPRS Support Node*) est l'interface logique entre un abonné GSM et le réseau de données externe. C'est un routeur, il assure le routage des données et la gestion de la mobilité (enregistrement des abonnés, authentification du mobile droit d'accès, taxation...) ;

– le **GGSN** (*Gateway GPRS Support Node*) est le routeur d'accès aux autres réseaux de données.
– un **RGPRS** (*Register GPRS*) est une base du type HLR dédié aux réseaux GPRS pour la gestion et la localisation des abonnés.

Le réseau GPRS offre un débit maximal de 114 kbit/s. Il est perçu comme une solution transitoire dans l'attente des réseaux multimédias de la troisième génération devant offrir des débits allant jusqu'à 2 Mbit/s (**UMTS**, *Universal Mobile Telecomminication System*).

15.5.6 La mobilité et l'accès à Internet

Une nouvelle génération de téléphones portables « embarque » un navigateur allégé. Le protocole en mode circuits (GSM) ou mode paquets (GPRS) **WAP** (*Wireless Application Standard*) autorise l'accès à Internet depuis un portable. Le débit réduit et la non-convivialité du terminal pénalise le développement du WAP.

Le WAP est un ensemble de protocoles permettant l'accès aux pages Web à partir d'un navigateur embarqué. La pile protocolaire représentée figure 15.43 est une adaptation de l'architecture TCP/IP aux contraintes des réseaux radios.

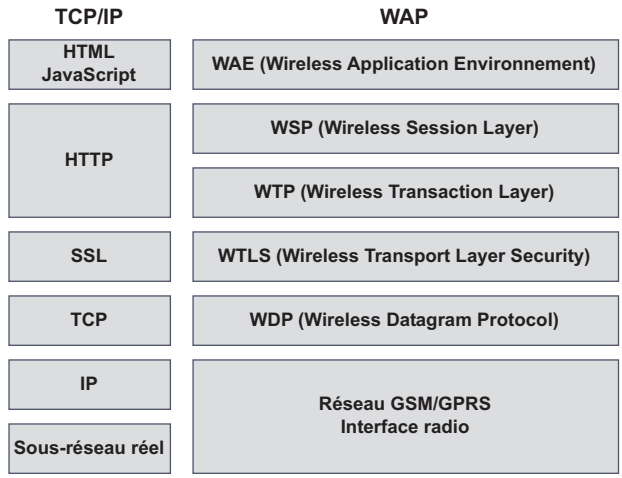


Figure 15.43 Empilement protocolaire du WAP.

L'utilisation d'un navigateur allégé et d'un langage spécifique le **WML** (*WAP Markup Language*) dérivé de **XML** (*eXtensible Markup Language*) nécessite d'utiliser une passerelle de conversion pour assurer l'adaptation des requêtes et des formats (figure 15.44).

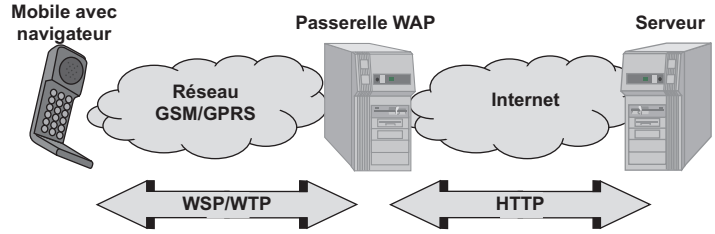


Figure 15.44 Transfert d'une requête WAP.

© Dunod – La photocopie non autorisée est un délit

Les Japonais utilisent un système similaire dit **i-Mode**. Le langage i-Mode étant directement dérivé de HTML, le service i-Mode ne nécessite pas l'utilisation de passerelle de compression de contenu. S'appuyant directement sur des réseaux GSM et GPRS, il demande peu de développement d'infrastructure, il constitue l'offre de Bouygues Télécom.

15.5.7 Évolution des systèmes de téléphonie mobile, l'UMTS

En intégrant à l'origine les services multimédias à haut débit (2 Mbit/s), l'**UMTS** constitue l'évolution naturelle des systèmes de communication entre mobiles.

Les bandes de fréquences allouées à l'UMTS se situent autour des 2 GHz avec une largeur de bande de 230 MHz. L'accès au canal utilise la technique du **W-CDMA** (*Wide band CDMA*). Les débits offerts à une station sont directement en relation avec la taille d'une cellule :

– de 144 à 384 kbit/s en zone rurale pour des mobiles dont la vitesse de déplacement est inférieure à 500 km/h (TGV) ;
– de 384 à 512 kbit/s en zone urbaine pour des vitesses de déplacement inférieures à 120 km/h ;
– jusqu'à 2 Mbit/s à moins de 10 km de la base radio.

Les chiffres ci-dessus s'entendent pour une utilisation du système en extérieur. Compte tenu des fréquences utilisées, les systèmes de téléphonie mobile sont en principe des systèmes *outdoor*, c'est-à-dire des systèmes destinés à être utilisés en extérieur.

15.5.8 La téléphonie satellitaire

Du géostationnaire aux constellations de satellites

Le premier réseau de communication pour mobiles utilisant des liens satellites date de 1982 (Immarsat A). Le réseau utilise quatre satellites géostationnaires et environ 40 stations terrestres. Il couvre l'intégralité de la surface du Globe sauf les pôles. Immarsat offre un service de téléphonie (voix, fax), de messagerie (messages courts du type *pager*) et de données (débit de 2,4 kbit/s à 64 kbit/s). Immarsat E est couplé au **GPS** (*Gobal Positionning System*), il offre un service de positionnement pour les navires en détresse (balise Argos).

Le système Immarsat n'intéresse qu'un segment très réduit de clientèle. En effet, des terminaux de plusieurs kilogrammes, des antennes de 80 à 90 cm et la nécessité de « viser » le satellite réservent ce système de communication à des usages professionnels (navires...)

En orbite géostationnaire (36 000 km), le temps bouche/oreille est de 240 ms minimum ce qui introduit une gêne dans l'interactivité des communications, d'où de nombreux projets reposant sur l'utilisation de satellites défilant en orbite basse.

Les systèmes à orbite basse

➤ Le système Iridium

D'origine Motorola, le projet initial de 77 satellites (d'où le nom du 77^{e} élément de la classification de Mendelïev), Iridium a été réduit à 66 satellites répartis sur 6 plans orbitaux en orbite basse à environ 780 km d'altitude (**LEO**, *Low Earth Orbital*). Après une mise en service

et un arrêt immédiat faute d'abonné, Iridium a été remis en service en mars 2001. Il offre des services de voix, données, fax et messagerie.

L'une des particularités essentielles d'Iridium est de permettre une communication intersatellite : les communications, entre deux mobiles, peuvent être acheminées directement dans le réseau Iridium sans emprunter de liens terrestres. Les communications sont établies en *full duplex* à 2,4 kbit/s (bande passante identique pour la transmission de données et les fax).

➤ Le système Globalstar

Globalstar, soutenu par Alcatel et France Télécom, utilise 48 satellites en orbite basse (1 410 km) répartis sur 8 plans orbitaux. À la différence d'Iridium les communications intersatellites ne sont pas possibles. Pour mettre en relation deux utilisateurs non desservis par le même satellite, Globalstar utilise les réseaux traditionnels des opérateurs terrestres.

Globalstar offre les mêmes services qu'Iridium mais autorise, en plus, une fonction de localisation de type GPS. Chaque satellite peut établir 28 800 communications simultanées.

15.6 CONCLUSION

Phénomène de ce début de XXI^{e} siècle, la mobilité envahit tous les domaines des télécommunications. Que ce soit en milieux professionnels ou privés la connectivité des équipements et leur communication feront vraisemblablement l'objet de développements et d'applications que l'on ne peut encore imaginer.

© Dunod – La photocopie non autorisée est un délit

EXERCICES

Exercice 15.1 Capacité d'un commutateur

La capacité d'un autocommutateur d'un opérateur de téléphonie est de 5 000 erlangs. Ce commutateur dessert des abonnés résidentiels et professionnels à concurrence de 40 et 60 %. On sait en outre, qu'un professionnel a un trafic à l'heure de pointe 3 fois supérieures à celui d'un abonné résidentiel qui est supposé de 0,1 erlang. On demande, quel est le nombre total d'abonnés desservis si la capacité du commutateur est utilisée à 100 % ?

Exercice 15.2 Itinérance

Lors d'un changement de cellule, votre communication téléphonique est interrompue alors que d'autres personnes déjà présentes dans la nouvelle cellule poursuivent leur communication. Quelle peut être la raison de cette interruption ?

Exercice 15.3 Système Iridium

Si la durée de révolution d'un satellite Iridium est de 100 mn, quel est le temps moyen pendant lequel un poste terrestre mobile qui ne se déplace pas sera pris en compte par un même satellite ?

Exercice 15.4 Schéma de réutilisation des fréquences

Un système de téléphonie cellulaire dispose de 240 fréquences, sachant que les cellules ont un profil hexagonal et qu'une même fréquence ne peut être réutilisée dans une cellule adjacente, quel est le nombre de fréquences disponibles pour une cellule (accès FDMA) ?

Exercice 15.5 Protocole D (Q.931)

La trace reproduite ci-dessous correspond au renvoi du terminal actif vers le terminal 01 23 45 67 89. L'analyseur a décodé les messages LAP-D, et fourni la signification et le contenu du champ d'information (protocole D). Il vous est demandé d'indiquer, pour chacun des messages, la signification des éléments d'information.

L	Horodatage	Origine	SAPI	TEI	C/R	Type	Contenu du message
1	01:06:34–678	Net	0	127	1	UI	Orig Q.931 Etablissement
			Mode de fct support				: 80 90 A3
			Identification canal				: 81
			Comp. Couches sup				: D1 81
2	01:06:34–714	Usr	0	64	0	SABME	
3	01:06:34–885	Net	0	64	0	UA	
4	01:06:34–933	Usr	0	64	0	INFO	Dest Q.931 Libération
			Cause				: 87 90
			Facilités				: 00 2A 32 32 23
			Mode de fct usager				: 80
			Numéro appelé				: 80 30 31 32 33 34 35 36 37 38 39
5	01:06:34–974	Net	0	127	0	RR	

Nota : dans les traces « L » représente le numéro de ligne auquel il est fait référence dans les corrections.

Chapitre **16**

Installation d'abonné et réseau privé de téléphonie

16.1 LES AUTOCOMMUTATEURS PRIVÉS

16.1.1 Généralités

Un autocommutateur privé de téléphonie, **PABX** (*Private Automatic Branch eXchange*) est l'interface entre le service de téléphonie de l'entreprise et le réseau téléphonique (public ou privé). Sa fonction essentielle consiste à mettre, temporairement, en relation deux usagers (commutation de circuits). Cette relation peut être interne à l'établissement ou établie à travers le réseau téléphonique public (RTC ou RNIS) ou privé.

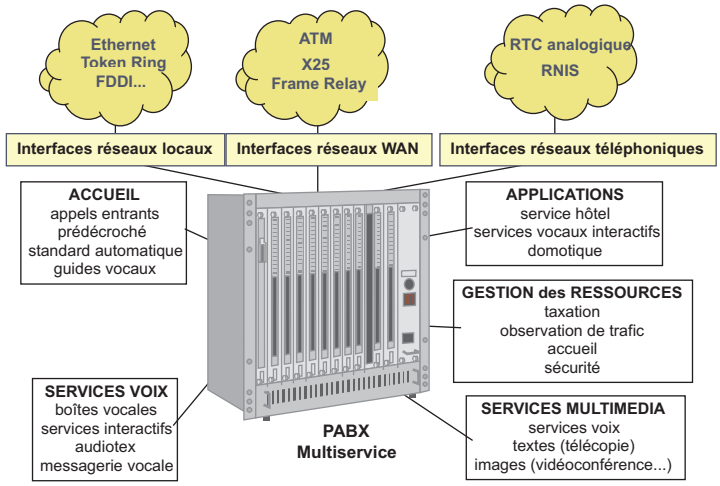


Figure 16.1 Le PABX au cœur des services d'entreprise.

La variété des services offerts par les PABX conduit à les intégrer de plus en plus au système d'information de l'entreprise. La figure 16.1 illustre la richesse fonctionnelle des PABX numériques multiservices de dernière génération.

16.1.2 Architecture d'un PABX

Un PABX numérique comporte essentiellement un réseau de connexion (commutation temporelle) qui établit, sous le contrôle de l'unité de contrôle (UC), une connexion temporaire entre le demandeur et le demandé. Cette connexion est établie en fonction de données usager (droits de l'usager, restrictions diverses, facilités offertes...). La figure 16.2 illustre l'architecture simplifiée d'un PABX.

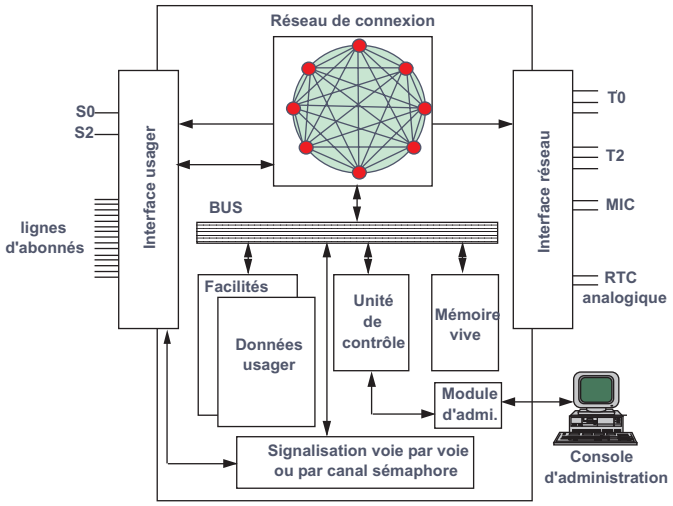


Figure 16.2 Architecture interne d'un PABX.

L'analyse de la numérotation est l'une des tâches essentielles du logiciel de gestion des PABX. La numérotation permet à l'unité de contrôle :

– de mettre en relation un usager demandeur et un usager demandé (correspondance entre un numéro logique – numéro d'appel – et un port physique de l'interface usager) ;

– de diriger l'appel vers telle ou telle ligne extérieure (préfixe de prise de ligne) ;

– d'accorder à l'usager une certaine facilité (renvoi, verrouillage du poste...).

L'ensemble des règles de gestion, en relation avec la numérotation, constitue **le plan de numérotation**.

16.1.3 Les téléservices et applications vocales offerts par les PABX

Les téléservices

Les techniques numériques, mises en œuvre dans les autocommutateurs numériques, ont permis d'offrir aux utilisateurs des services complémentaires facilitant, ainsi, la communication

générale dans l'entreprise. Les services supportés dépendent essentiellement du constructeur. Cependant, les facilités de base sont implémentées sur tous les systèmes. Ce sont notamment :

- les techniques de renvoi (renvoi immédiat, renvoi sur non-réponse ou renvoi différé, renvoi sur occupation) ;
- la supervision et le filtrage des postes (relation secrétaire/patron) ;
- le multitouche qui autorise la prise d'un second appel et le double appel. Ces deux facilités permettent le va-et-vient entre les correspondants et la conférence à trois ;
- le multiligne c'est-à-dire plusieurs lignes chacune dotée du même numéro (mono-annuaire) ou de numéros différents (multiannuaire) ;
- les groupements d'interception, ensemble d'utilisateurs réunis en un groupe de communication. Toute communication, à destination d'un membre du groupe, peut être interceptée par tout membre du groupe ;
- l'annuaire collectif qui autorise notamment l'appel par le nom et chez l'appelé l'affichage du nom de l'appelant. Certains constructeurs proposent un annuaire extérieur. Cette facilité permet, lors des appels entrants de substituer au numéro d'appelant un nom ;
- la numérotation abrégée collective ou personnelle ;
- le rappel automatique sur poste occupé. Cette facilité permet le rappel automatique d'un correspondant occupé lorsque celui-ci aura terminé la communication en cours ;
- le transfert d'appel au sein de l'entreprise ou vers l'extérieur, si cette dernière facilité est autorisée ;
- les groupes de diffusion : cette technique permet de diffuser, à partir d'un poste maître, un message sur un ensemble de postes téléphoniques sans que les correspondants aient décroché (recherche de personnes, messages de sécurité...) ;
- l'interphonie (mise en relation d'usager sans décrochage du poste).

L'usage de ces facilités ne s'est véritablement développé qu'avec l'apparition des postes numériques[1] avec afficheur et touches programmables.

Les applications vocales

Ces applications ont pour objet de faciliter les relations de l'entreprise avec le monde extérieur. Parmi ces applications, la plus utilisée est la **messagerie vocale**. Celle-ci permet à un correspondant de déposer un message pendant l'absence de l'appelé (service de communication différée).

Le **standard automatique** substitue à l'opératrice un ensemble de guides vocaux acheminant l'appel vers le destinataire lorsque le numéro de celui-ci n'est pas connu ou n'est pas diffusé (service de mise en relation automatique). Cette application peut véritablement faciliter l'acheminement des appels, mais elle doit faire l'objet d'une étude sérieuse pour éviter

1. Attention, il ne faut pas confondre poste numérique et poste Numéris. Ces derniers sont étudiés pour être raccordés directement au réseau Numéris (interface So). Les premiers, généralement beaucoup plus riches en fonctionnalité, sont spécifiques à un constructeur, on les appelle aussi postes dédiés.

© Dunod – La photocopie non autorisée est un délit

d'avoir à parcourir une arborescence trop développée qui dissuade l'appelant. La figure 16.3 illustre le mécanisme du standard automatique.

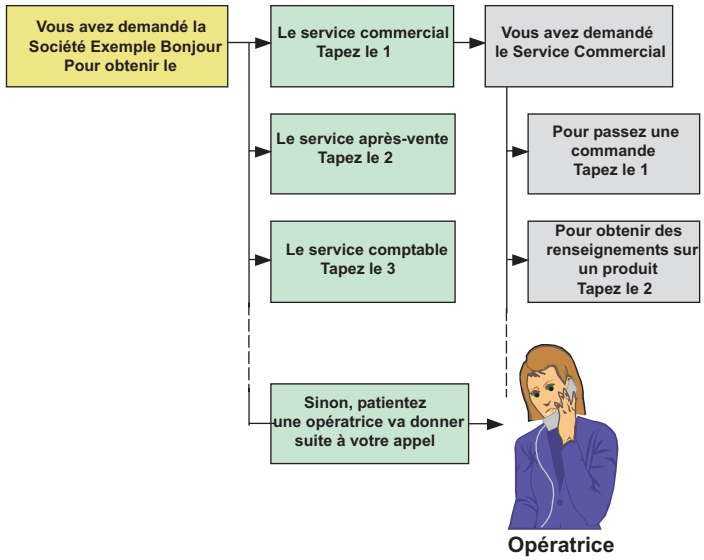

Vous avez demandé la Société Exemple Bonjour Pour obtenir le
Le service commercial Tapez le 1
Vous avez demandé le Service Commercial
Le service après-vente Tapez le 2
Pour passez une commande Tapez le 1
Le service comptable Tapez le 3
Pour obtenir des renseignements sur un produit Tapez le 2
Sinon, patientez une opératrice va donner suite à votre appel
Opératrice

Figure 16.3 Principe du standard automatique.

Les **serveurs audiotex** permettent l'automatisation du traitement des demandes répétitives d'information. Fondés sur le même principe que les standards automatiques, les serveurs audiotex sont constitués d'une série de guides vocaux qui conduisent l'utilisateur, à travers une arborescence, vers le renseignement qu'il désire obtenir (service de diffusion d'information).

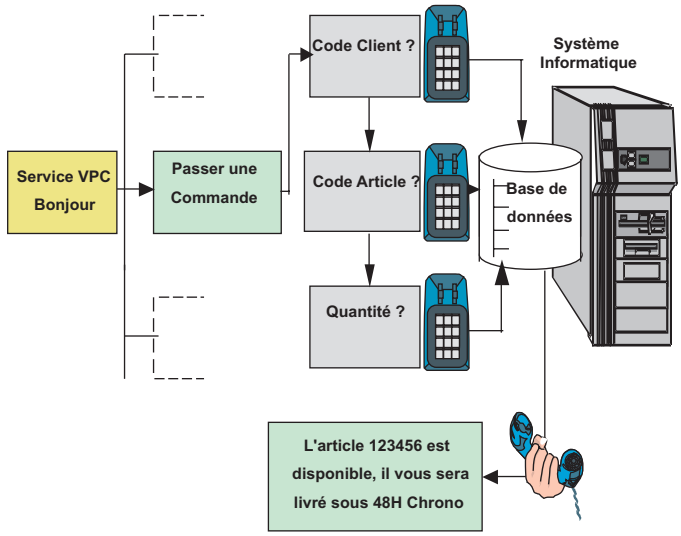


Figure 16.4 Exemple d'application sur serveur vocal interactif.

Les **serveurs vocaux interactifs** ont pour objectif l'automatisation du traitement de demandes répétitives d'informations par des transactions personnalisées. La première

application est, par exemple, utilisée par les organismes bancaires pour informer leurs clients sur l'état de leur compte. La seconde utilise les postes téléphoniques comme terminal de saisie d'une application informatique. Ce service, généralement mis en œuvre par les sociétés de vente par correspondance, est illustré par la figure 16.4.

Ces diverses applications nécessitent de disposer d'un poste multifréquences (**DTMF**, *Dual Tone MultiFrequency*) et d'associer une commande à une touche. Les fréquences audios sont transmises en transparence sur la liaison (RTC) ou dans l'IT voix (canal B du RNIS).

Intégration Téléphonie/Informatique

➤ Le CSTA (Computer Supported Telephony Applications)

Ayant pour origine les travaux de DEC, le concept de **CTI** (*Computer Telephony Integrated*) organise les échanges entre un PABX et un ordinateur. Il a donné naissance à la norme CSTA publiée par l'ECMA dont le concept est illustré figure 16.5.

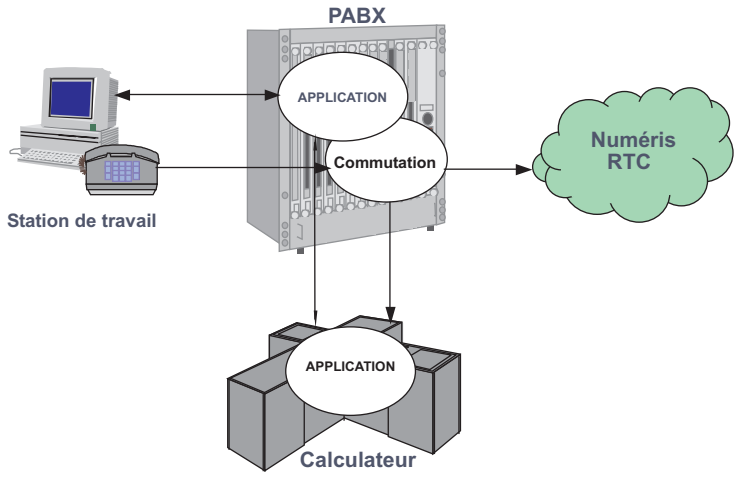


Figure 16.5 Principe du CSTA.

La recommandation CSTA organise le dialogue de la couche application du modèle OSI entre un serveur CTI et un PABX. Elle décrit un ensemble de services, mais ne précise aucune **API** (*Application Programming Interface*), contrairement au concept *CallPath* d'IBM qui spécifie un service d'API conforme à l'architecture SAA d'IBM. S'appuyant sur les principes du RNIS et notamment de la signalisation SS7, CSTA cantonne le PABX aux fonctions de commutation de circuits et reporte les fonctions intelligentes sur l'ordinateur.

L'association ordinateur/téléphonie devrait connaître un développement important, surtout dans l'accueil téléphonique. Dans l'exemple de la figure 16.6, l'ordinateur exploite le numéro d'appelant et affiche automatiquement, avant que le poste n'ait décroché, les informations relatives au demandeur, sur l'écran de l'ordinateur.

➤ Les API TAPI et TSAPI

D'origine Microsoft, les API (figure 16.7) **TAPI** (*Telephony Application Programming Interface*) ou Novell et AT & T **TSAPI** (*Telephony Services Application Programming Interface*)

© Dunod – La photocopie non autorisée est un délit

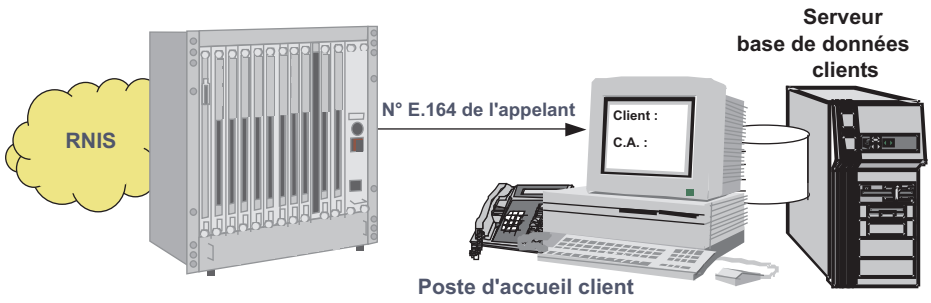


Figure 16.6 Principe d'un accueil fondé sur CSTA.

permettent de développer, sur micro-ordinateur, des applications qui accèdent, au moyen de la souris et du clavier, aux fonctions essentielles du PABX telles que :

– l'annuaire et la numérotation automatique,
– l'interception d'appel,
– la supervision de poste,
– la consultation de messagerie,
– l'établissement de statistiques téléphoniques personnelles.

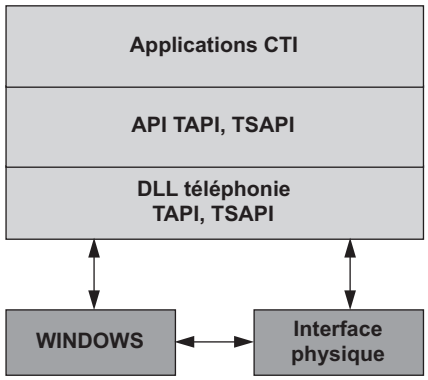


Figure 16.7 Architecture générale du concept CTI sur micro-ordinateur.

TSAPI et TAPI ont des fonctionnalités similaires mais adoptent des approches différentes (convergence avec TAPI 2.0). TSAPI distribue les services téléphoniques sur le réseau local via un serveur de téléphonie. TAPI relie directement le poste de travail à l'autocommutateur (figure 16.8).

Une API Java, JTAPI permet aux applications développées en Java d'accéder aux services téléphoniques et de les enrichir de nombreuses fonctionnalités informatiques. JTAPI s'appuie sur les API TSAPI et TAPI.

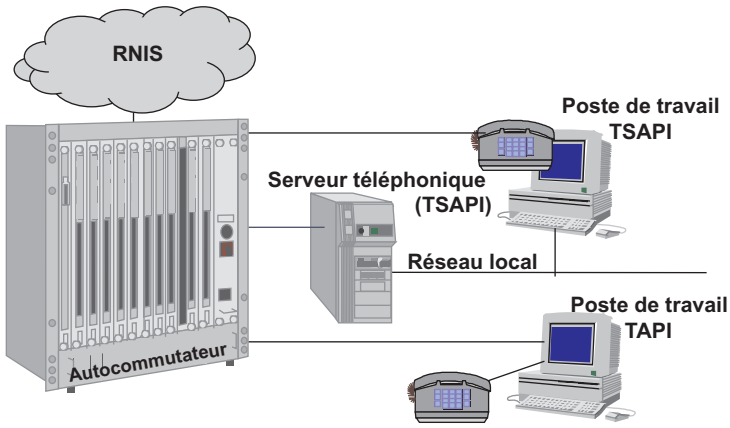


Figure 16.8 Principe général de TSAPI et de TAPI.

La visiophonie

Ce n'est qu'avec l'apparition du RNIS et de ses canaux B à 64 kbit/s que la transmission simultanée de l'image et de la voix a été réalisable. Cependant, l'expérience de Biarritz (1986), avec quelque 1 500 foyers raccordés, a conduit, pour des raisons économiques, à l'abandon de la généralisation de ce service.

La visiophonie reste aujourd'hui limitée à la communication au sein de l'entreprise. Le poste visiophone est composé d'une caméra et d'un écran intégré au poste téléphonique. Associée à un micro-ordinateur, la visiophonie permet l'affichage de l'image dans une fenêtre *Windows*.

Une série de normes, regroupées dans la recommandation H.320, régit la compression de l'image et de la voix, la transmission des informations et la signalisation d'usager à usager. Elle détermine les conditions d'interfonctionnement des terminaux de visiophonie.

Normes	Objet
Codage et décodage des images animées	
H.261	Autorise des débits multiples de 64 kbit/s (appelé encore norme P64 avec $1 \leqslant p \angle 31$
Gestion du système et signalisation	
H.221	Multiplexage et démultiplexage de 1 à 6 canaux B
H.230	Pour le contrôle et l'identification
H.242	Pour la communication et la reconnaissance entre deux terminaux
H.321	Pour la définition et la structure des trames
Codage et décodage du son	
G.711	Son de qualité normale 3,4 kHz numérisé à 64 kbit/s
G.722	Son de qualité supérieure à 7 kHz numérisé à 64 kbit/s
G.728	Son de qualité normale 3,4 kHz compressé à 16 kbit/s
Services associés	
H.233	Codage des sécurités
T.120	Gestion des transferts de fichiers sur le RNIS

Figure 16.9 Principales normes de la visiophonie.

© Dunod – La photocopie non autorisée est un délit

Cet ensemble de normes assure le partage de 1 à n canaux B. La qualité et les modalités de compression d'image sont principalement définies par les normes **CIF** (*Common Intermediate Format*, 352 points, 288 lignes) et **QCIF** (*Quarted Common Intermediate Format*, 176 points et 144 lignes).

Le codeur (Codec H.261) effectue une prédiction temporelle (estimation du mouvement par bloc de 8x8 pixels dans un espace de 47x47 pixels). Seule, la différence entre l'image prédite et l'image réelle est codée et transmise. La figure 16.9 cite les principales normes utilisées par la visiophonie.

16.1.4 PABX et transmission de données

Au centre de la communication d'entreprise, les constructeurs de PABX ont très vite intégré à leur autocommutateur des fonctionnalités données (figure 16.10). La numérisation des PABX et la mise à disposition d'interface LAN (Ethernet, Token Ring...) ont engendré la banalisation du câblage et autorisé une véritable interconnexion des LAN via un lien numérique ou des liens MIC (interface G.703, G.704). Ce dernier moyen, réalisant, via une régie, l'agrégation de n canaux de 64 kbit/s constitue les prémices d'une intégration voix/données (IT[2] voix et IT données sur le même support).

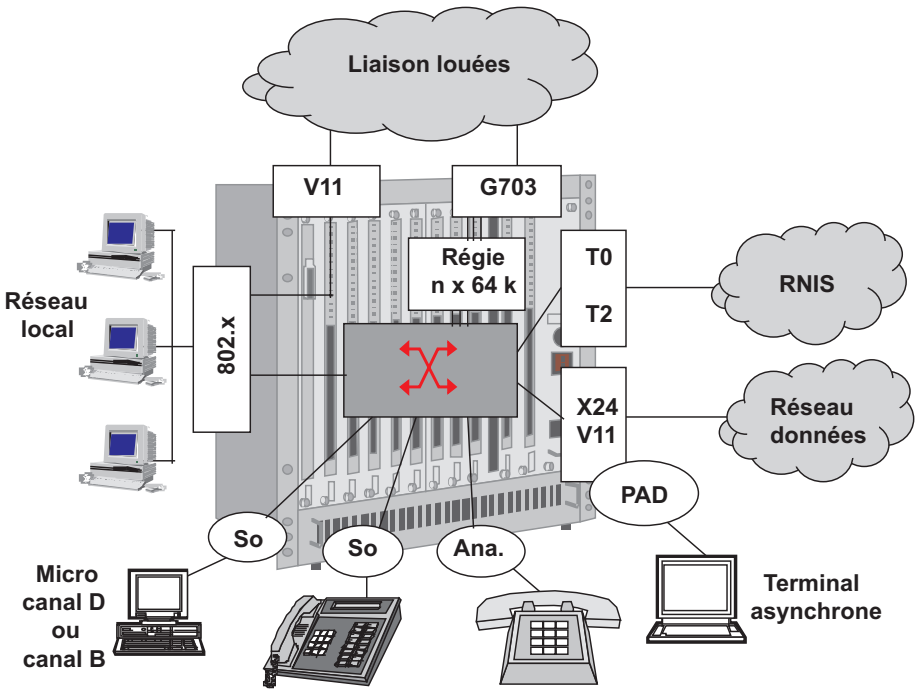


Figure 16.10 Le PABX et la transmission de données.

2. IT, intervalle de temps.

La mise à disposition d'accès X.25 via les canaux D (9,6 kbit/s) et B (64 kbit/s) a doté l'autocommutateur de fonctionnalités de commutateur de paquets X.25. Cependant, les besoins voix et données n'ont pas une évolution similaire. De ce fait, les investissements sont restés désynchronisés, et le PABX traditionnel n'a pas réussi à devenir le nœud de communication voix, données et images de l'entreprise. Les techniques sont restées disjointes.

Si la convergence voix/données n'a pas eu lieu par la voix, les réseaux données ont réussi cette intégration (voir section 16.4).

16.2 L'INSTALLATION D'ABONNÉ

16.2.1 Généralités

L'installation de téléphonie privée prolonge dans l'entreprise les services téléphoniques du réseau public. La définition d'une installation téléphonique comporte trois phases (figure 16.11). Les deux premières d'ordre technique consistent à dimensionner l'installation (équipement local, raccordement au réseau public). La troisième, d'ordre organisationnel, cherche à définir les services à offrir aux utilisateurs.

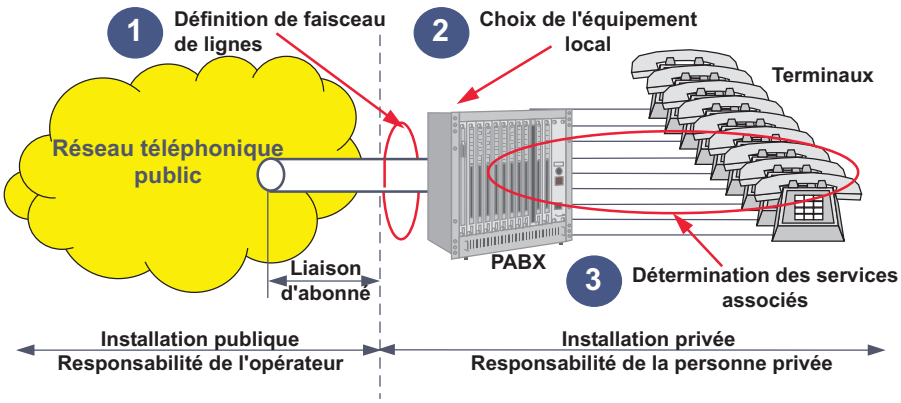


Figure 16.11 Définition de l'installation de téléphonie privée.

Le choix de l'équipement local est essentiellement dicté par la nature des services à offrir aux utilisateurs, du nombre de postes à raccorder et de la puissance de commutation nécessaire. Le dimensionnement du PABX nécessite d'estimer le trafic à écouler, ce trafic s'exprime en erlang[3]. Il est en relation directe avec la nature de l'entreprise, un centre d'appel demande, pour un même nombre de postes, une puissance de commutation plus importante qu'un établissement industriel. À défaut de renseignement statistique sur le trafic téléphonique d'une entreprise, on formule l'hypothèse suivante (valeurs statistiques admises par la profession) : le trafic d'un poste, à l'heure de pointe, est évalué à 0,12 erlang se répartissant comme suit :

– 0,04 erlang en trafic sortant,
– 0,04 erlang en trafic entrant,
– 0,04 erlang en trafic interne à l'entreprise.

3. Rappelons que l'erlang mesure l'intensité de trafic.

© Dunod – La photocopie non autorisée est un délit

16.2.2 Dimensionnement du raccordement au réseau de l'opérateur

Spécialisation des lignes

On appelle liaison d'abonné, la ligne entre le réseau public (commutateur de rattachement) et l'installation d'abonné. On distingue trois types de lignes (figure 16.13) :

– les lignes **SPA** (Spécialisées arrivée Point A), ce sont des lignes qui ne peuvent acheminer que des appels sortants (vers le réseau de l'opérateur ou point A) ;

– les lignes **SPB** (Spécialisées arrivée Point B), ce sont des lignes qui ne peuvent acheminer que des appels entrants (vers l'installation d'abonné ou point B) ;

– les lignes **mixtes**, ce sont des lignes qui acheminent indifféremment les appels entrants ou sortants, elles sont à la fois SPA et SPB.

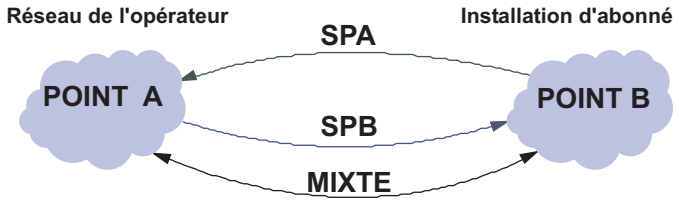


Figure 16.12 Les différents types de lignes.

On désigne par faisceau un ensemble de lignes de mêmes caractéristiques (faisceau de lignes SPA, faisceau de lignes SPB ou faisceau de lignes mixtes).

La spécialisation des lignes interdit la saturation des lignes par un type d'appel. L'entreprise favorise ainsi les appels entrants (clients) par la limitation des appels sortants (personnel de l'entreprise). Les appels sortants sont limités par le nombre de SPA. Dans une telle conception, les lignes mixtes sont généralement vues comme des lignes de débordement.

Dans ce cas, l'abonnement comporte trois faisceaux, un faisceau SPA, un faisceau SPB et un faisceau de débordement (ou mixte). Le raccordement d'un tel abonnement à l'autocommutateur local (PABX) doit être correctement effectué si l'on veut que le faisceau mixte joue son rôle de gestion du trafic de débordement.

En effet, compte tenu qu'un autocommutateur adresse les appels sortants sur la première ligne sortante trouvée libre si, dans l'autocommutateur les mixtes sont définies en premier, elles seront attribuées par celui-ci en premier et ne joueront plus leur rôle de gestion du trafic de débordement. La tête de groupement doit donc être définie en SPB, puis SPA et enfin les lignes mixtes.

Dimensionnement des faisceaux de lignes

Généralement la potentialité d'appels simultanés (n) est supérieure aux ressources disponibles (m). Dans ces conditions, l'appel $m+1$ sera refusé. Le dimensionnement d'un faisceau consiste à déterminer en fonction du trafic à écouler et d'une probabilité de refus par manque de ressource quel est le nombre de circuits nécessaires. Erlang a établi que la probabilité p de refus d'appel, appelé aussi facteur de blocage, par suite d'encombrement pour un trafic à écouler de

E erlang dans un système possédant m lignes est donnée par la relation :

$$p = \frac{E^m/m!}{\sum_{k=0}^{k=m} E^k/k!}$$

Cette formule a permis d'établir des abaques de dimensionnement appelés abaques d'Erlang, dont une forme est représentée figure 16.13.

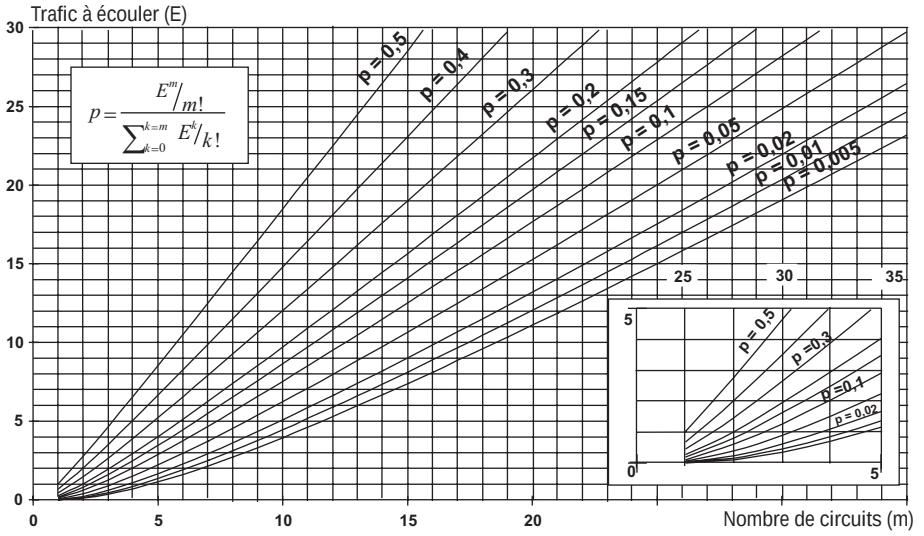


Figure 16.13 Abaque d'Erlang (modèle à refus).

Le dimensionnement consiste à affecter à chaque faisceau un nombre de lignes suffisant pour écouler un certain trafic (exprimé en erlang) avec une certaine qualité de service. La méthode a été abordée au chapitre 7 (section 7.1.2). Appliquée à la téléphonie la définition du faisceau consiste, généralement, à déterminer le nombre de lignes SPA et SPB dans des conditions de services différentes.

En principe, dans les entreprises les appels sortants et entrants subissent un traitement différent. Les appels sortants, ceux du personnel vers l'extérieur, sont refusés en cas de manque de ressource. En ce qui concerne les appels entrants (ceux des clients), ils peuvent être refusés par manque de ressource (ligne disponible), mais aussi mis en attente lorsque le correspondant demandé est déjà en communication. Ce procédé monopolise une ressource en arrivée et n'écoule aucun trafic. Dans ces conditions, la probabilité p_a pour qu'un nouvel appel entrant soit refusé par manque de ressource est plus importante. Cette probabilité est donnée par la relation (modèle dit à attente) :

$$p_a = \frac{\left(E^m/m!\right) \cdot \left(\dfrac{m}{m-E}\right)}{\left[\sum_{k=0}^{k=m-1} E^k/k!\right] + \left[\left(E^m/m!\right) \cdot \left(\dfrac{m}{m-E}\right)\right]}$$

© Dunod – La photocopie non autorisée est un délit

Généralement, les lignes SPA sont définies selon le modèle à attente et les lignes SPB selon le modèle à refus. Notons que le modèle d'Erlang est un modèle pessimiste, le nombre de lignes sera toujours arrondi au nombre entier inférieur.

16.3 LES RÉSEAUX PRIVÉS DE PABX

16.3.1 Principes généraux

La volonté de maîtriser les coûts et d'harmoniser, au sein de l'entreprise, l'ensemble des services à conduit les responsables télécoms des entreprises à réaliser l'interconnexion de leur parc de PABX (Réseaux Privés à Intégration de Services ou **RPIS**).

Interconnecter deux ou plusieurs PABX consiste à les relier par un ensemble de liens privés (faisceau) ou publics loués afin d'acheminer, à partir de l'un les appels destinés à l'autre et inversement, sans passer par le réseau (figure 16.14).

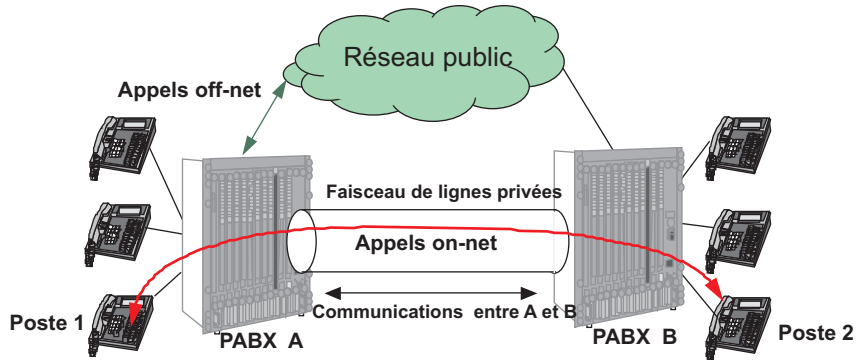


Figure 16.14 Principe d'un réseau privé de PABX.

Dans ce type de réseau, un préfixe (souvent le 0) permet d'identifier les appels destinés à être acheminés par le réseau public (**appels off-net**). Les appels internes au réseau (**appels on-net**) sont établis en utilisant un plan de numérotation propre à l'entreprise. Une table, dite table d'acheminement, configurée manuellement dans chaque PABX, achemine l'appel vers le faisceau qui relie le PABX de l'appelant au PABX de l'appelé.

Généralement, la numérotation interne à l'entreprise utilise les quatre derniers chiffres du numéro SDA (MCDU[4]) de l'entreprise. Les numéros publics (série SDA) sont fournis par l'opérateur, l'entreprise n'a aucune maîtrise sur les numéros accordés. Dans ces conditions, il est non seulement difficile mais aussi dangereux (changement de séquence SDA) de réaliser une numérotation homogène à partir de ces chiffres sur l'ensemble des sites constituant le réseau. Pour éviter d'adopter une numérotation interne différente de la numérotation externe (numéro interne différent du MCDU), chaque site est généralement identifié par un préfixe. La figure 16.15 présente un exemple de réseau utilisant un plan de numérotation global et homogène pour toute l'entreprise. Le préfixe 2*x* est utilisé pour distinguer les appels *on-net*

4. MCDU, Millier Centaine Dizaine Unité, désigne les quatre derniers chiffres du numéro E.164 de l'installation de l'abonné (ZZ ABPQ MCDU) ; SDA, Sélection Directe à l'Arrivée.

(*2x*) des appels *off-net* (préfixe 0). Dans notre exemple, le chiffre *2*, premier chiffre du préfixe indique un appel *on-net* et le deuxième chiffre (*x*) identifie le site distant.

Table d'acheminement du PABX 21

Numéro	Faisceau
22*	B
23*	E
24*	B
25*	A
22*	E
23*	B
...	

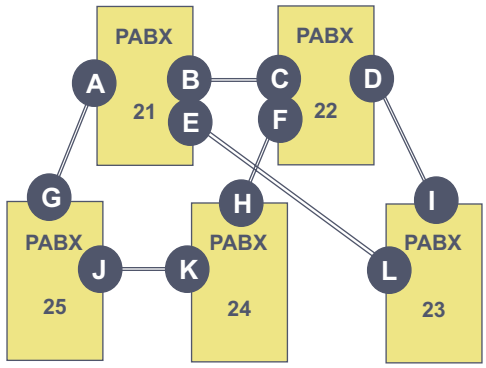


Figure 16.15 Principe d'un plan de numérotation privé.

En cas d'occupation d'un faisceau, un faisceau de débordement peut être spécifié. Par exemple, si toutes les lignes du faisceau B sont occupées, il est possible d'acheminer le trafic à destination du site 22 en transitant par le site 23 (faisceau E). Dans certains réseaux, pour garantir qu'un appel pourra aboutir (taux de service important), le réseau public peut être programmé comme faisceau de débordement. Dans ce cas, une table locale dite table de transformation de numérotation assure la traduction entre le numéro interne de l'appelé et son numéro sur le réseau public.

Lorsque l'un des PABX mis en réseau ne dispose d'aucun accès sur le réseau public, il est complètement asservi à un autre PABX du réseau. Il ne constitue alors qu'une simple unité de raccordement déportée (**URAD**). Cette relation entre deux PABX est dite siège/satellite. C'est l'ordinateur siège qui gère les communications (restrictions utilisateurs...) et établit la taxation.

Indépendamment des économies réalisées par la gratuité des communications internes au réseau, une économie sur les appels « longue distance » vers des usagers n'appartenant pas au réseau peut être réalisée en confiant, au PABX le plus proche de l'appelé, le soin d'établir la communication. La communication, demandée par le PABX B de la figure 16.16 vers un abonné du réseau public en zone de taxation locale du PABX A, conduit à la facturation au PABX A d'une communication locale en lieu et place d'une communication longue distance au PABX B.

Cette technique est dite **aboutement de réseaux** (mise bout à bout du réseau privé et du réseau public), la communication en aboutement (appels *on-net/off-net*) peut être réalisée par analyse complète de la numérotation de l'appelé et recherche du PABX le plus proche de l'appelé (fonction de routage au moindre coût ou *Least Cost Routing*) ou préprogrammé dans chaque PABX par création d'un abonné fictif sur le PABX qui doit établir la communication vers le réseau public. Le correspondant est alors désigné par un numéro interne au réseau et non par son numéro public, seuls peuvent être appelés les correspondants préprogrammés.

La réalisation d'un réseau privé de PABX soulève les difficultés suivantes :

– détermination de la capacité du faisceau d'interconnexion. Ce problème a été abordé et les méthodes de résolution (loi d'Erlang) ont été étudiées précédemment ;

– l'hétérogénéité des PABX, indépendamment des normes qui diffèrent d'un pays à un autre

© Dunod – La photocopie non autorisée est un délit

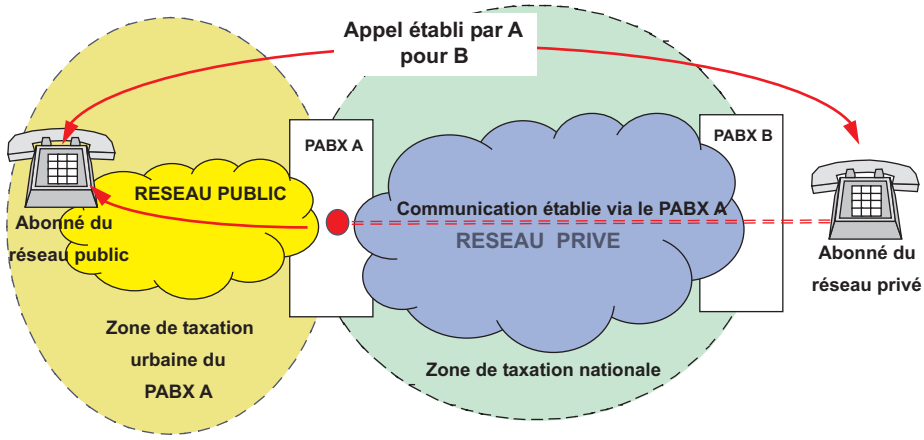


Figure 16.16 Principe de l'aboutement de réseau.

(raccordement, compression de la voix...), les constructeurs utilisent des protocoles de signalisation propriétaire et des services spécifiques. La réalisation d'un réseau de PABX se trouve généralement confrontée à un existant hétérogène. La qualité de service offerte aux utilisateurs est alors réduite au plus petit dénominateur commun ;

– le choix de la liaison, liaison analogique (**LIA**, Liaison Inter-Automatique) ou numérique (**MIC**). La première ne convient que lorsque le nombre de liens à établir entre deux sites est faible (2 à 3) et que les éléments à relier sont locaux.

16.3.2 La signalisation et type de liens

La signalisation téléphonique est constituée d'un ensemble d'informations décrivant l'état de la ligne (libre, occupée...), la numérotation (signal d'enregistreur) et éventuellement les téléservices associés. La signalisation peut être de type voie par voie (à chaque canal est associée une voie de signalisation) ou par canal sémaphore. La signalisation est alors commune à tous les canaux, elle est dite aussi signalisation en mode messages (exemple : SS7).

La signalisation voie par voie sur lien analogique

Le principe général des liaisons analogiques entre PABX (LIA, Liaison Inter-Automatique) est illustré par la figure 16.17. Les informations de voix et la signalisation sont séparées. La signalisation est dite **RON/TRON** (RéceptiON et TRansmissiON ou **E&M**, *Earth & Mouth*). Les fils voix sont généralement désignés fils AB. Une liaison LIA n'achemine qu'une communication téléphonique et la signalisation de cette communication (signalisation voie par voie). Il faut autant de LIA entre les PABX raccordés que de communications téléphoniques à écouler simultanément.

Dans ce schéma de principe, les informations d'état de la liaison comme par exemple la prise de ligne sont transmises par les fils RON/TRON. L'invitation à numéroter et le retour de sonnerie sont transmis sur les fils voix. Selon le nombre de fils utilisés, le mode de signalisation d'état (niveaux de tension, impulsions de tension, impulsions à 50 Hz...), on distingue quatre types de LIA :

– **LIA à changement d'état**, les différents événements sont signalés par le potentiel des fils RON et TRON. Des polarités permanentes sont maintenues pendant toute la durée de la communication sur les fils RON/TRON. La numérotation est transmise par coupure du fil TRON ou en numérotation multifréquentielle (Q.23) sur les fils voix ;
– **LIA à impulsions codées**, les différents événements sont représentés par des impulsions de 48 volts calibrées en durée. La durée de l'impulsion est significative de l'état à signaler, la prise de ligne est, par exemple, signalée par une impulsion de 100 ms. La numérotation est transmise par coupure du signal positif sur le fil TRON de l'émetteur (numérotation décimale) ou sur les fils voix (numérotation fréquentielle ou Q.23) ;
– **LIA à impulsions codées 50 Hz**, ce type de LIA n'utilise que 2 fils. La signalisation est transmise sous forme d'impulsions codées (50 Hz, 70 volts). De même, la numérotation est envoyée sous forme d'impulsions à 50 Hz (50/50 ms) ou en Q.23 ;
– **LIA à courant continu**, seuls deux fils sont utilisés. Ils servent à la parole et à la signalisation. Ce type de raccordement est en principe utilisé pour les liaisons d'abonnés. Les différents états (prise de ligne et libération) sont détectés par ouverture ou fermeture de la boucle de courant. La numérotation est décimale (impulsions de numérotation 66/33 ms) ou Q.23.

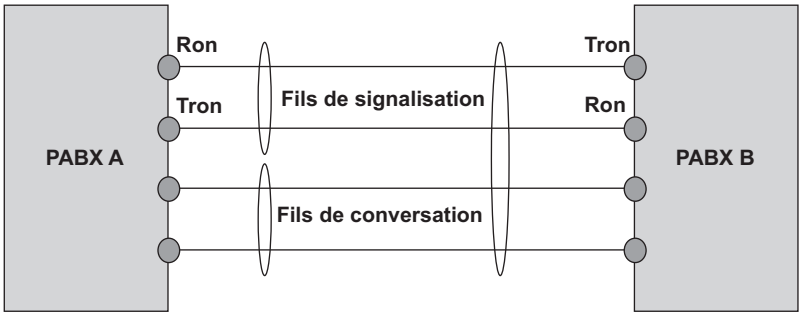


Figure 16.17 Principe d'une liaison LIA et de la signalisation RON/TRON.

Les LIA à changement d'état ou à impulsions codées peuvent être à 2 ou 4 fils RON/TRON et à 2 ou 4 fils conversation (2 fils conversation émission, notés fils CD et 2 fils de conversation réception, notés fils AB). Ces systèmes supportent la signalisation de type COLISEE[5] et SOCOTEL multifréquences (Q.23). La figure 16.18 illustre une liaison entre PABX réalisée à l'aide d'une LIA de type V.

En fonction de l'emplacement des sources d'alimentation (48 V) de la signalisation, les LIA sont classées en type (LIA de type I à V). Les LIA de type V sont les plus utilisées. Le passage de la liaison voix de 2 en 4 fils provoque, en cas de désadaptation d'impédance, un phénomène d'écho très perturbant qu'il conviendra d'éliminer. L'UIT prescrit l'utilisation de dispositifs d'annulation d'écho dès que le temps de transit dans le réseau est supérieur à 24 ms.

5. Ensemble de signaux (impulsions calibrées), d'origine France Télécom, décrivant tous les événements d'une communication téléphonique.

© Dunod – La photocopie non autorisée est un délit

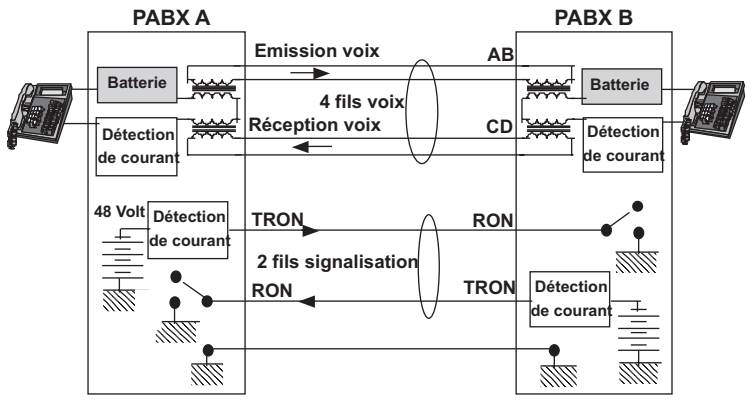


Figure 16.18 Liaison LIA à changement d'état de type V.

La signalisation voie par voie sur lien numérique

Le principe d'une liaison numérique est représenté par la figure 16.19. Une liaison de ce type comporte 4 fils (une paire émission et une paire réception). Chaque IT de la trame multiplexée est affecté à un canal voix. La signalisation de chaque voie (signalisation voie par voie) peut être transportée dans un IT dédié (signalisation hors bande) ou dans la même voie que la communication (signalisation dans la bande). Cette signalisation est dite **signalisation CAS** (*Channel Associated Signaling* ou signalisation par canal associé).

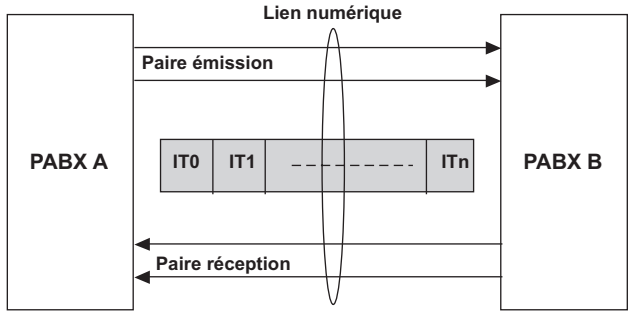


Figure 16.19 Principe d'une liaison numérique.

Deux types de trames multiplexées peuvent être utilisés. Elles diffèrent par le nombre d'IT qui les compose et le mode de signalisation utilisé :

– la trame européenne ou **E1** comporte 32 IT de 64 kbit/s. Couramment appelée trame MIC, elle assure un débit utile maximal de 1 920 kbit/s ;

– la trame nord-américaine (utilisée aussi au Japon) ou **T1** comporte 24 IT de 64 kbit/s pour un débit total de 1 544 kbit/s et utile de 1 536 kbit/s.

L'organisation de ces trames a été vue au chapitre 11, nous ne ferons ici qu'en rappeler le principe. La signalisation comporte deux types d'informations, celles relatives à la structure de la trame (ou signalisation de supervision) et celles en rapport avec l'état de chaque canal téléphonique (signalisation voie par voie ou CAS).

La trame de base T1[6] (trame G.733, aussi notée DS1 à DS12), représentée figure 16.20, comprend 24 IT (DS0) de 8 bits (192 bits). La multitrame de premier niveau regroupe 12 trames de base. Chaque trame de base est précédée d'un bit (bit de tramage constituant la signalisation de supervision). Ces 12 bits forment un mot (**mot SF**, *SuperFrame*) représentant la séquence binaire « 100011001100 » et identifiant la trame.

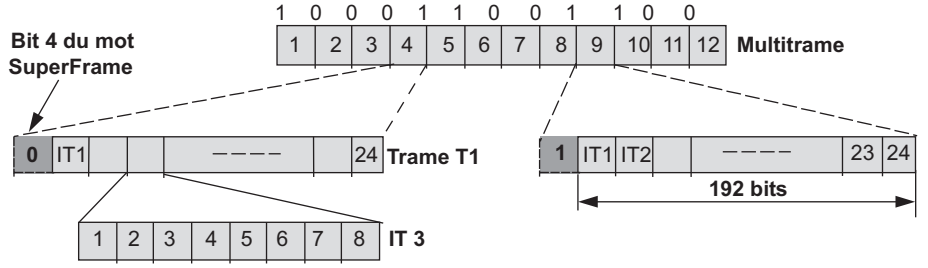


Figure 16.20 Organisation de la multitrame T1 (G.733).

La signalisation téléphonique de chacune des voies est réalisée par vol, toutes les 6 trames, du bit de poids faible dans l'IT voix correspondante (un bit de signalisation est substitué au bit d'information, c'est une signalisation dans la bande).

L'organisation de la trame E1 (G.732) est représentée figure 16.21. Elle comporte 32 IT dont 2 sont utilisés pour la signalisation (signalisation hors bande). L'IT0 de chaque trame est dédié à la supervision de la trame (identification du début de la trame et à la gestion de celle-ci). L'IT16 est utilisé pour la signalisation de chaque voie (signalisation CAS).

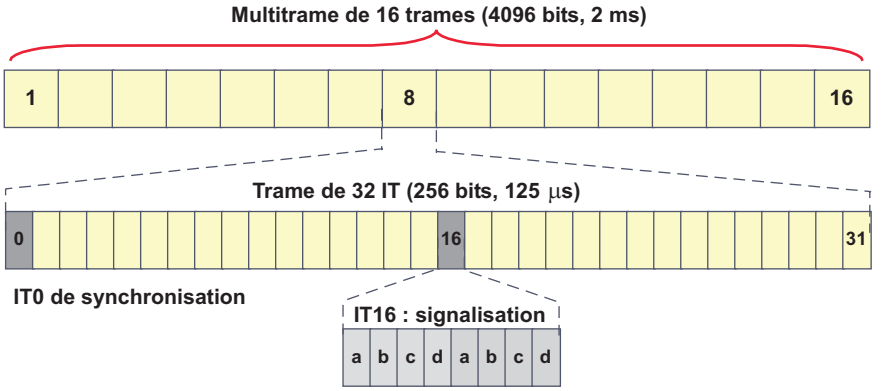


Figure 16.21 Organisation de la multitrame E1 (G.732).

La signalisation (figure 16.22) de chaque IT sur 4 bits (bit a, b, c et d) est transportée dans l'IT16 de chaque trame. Chaque IT16 transporte la signalisation de deux voies.

Mise en place lors de la transition de la téléphonie analogique vers la téléphonie numérique, la signalisation CAS traduit et transporte la signalisation analogique. De ce fait, elle ne comporte que les événements relatifs à la gestion de la ligne (prise de ligne, état occupé...). Une impulsion de la signalisation analogique est traduite par le positionnement à

6. T1 désigne le canal de transmission, DSx le format des données.

© Dunod – La photocopie non autorisée est un délit

TimeSlot 16 (IT 16)								
Trame 0	Trame 1		Trame 2		Trame n		Trame 15	
MVM Mot de Verrouillage Multitrame	abcd IT1	abcd IT17	abcd IT2	abcd IT18	abcd ITn	abcd ITn+16	abcd IT15	abcd IT31

Figure 16.22 L'organisation de l'IT 16.

1 du bit « *a* » durant 150 ms. Le tableau 16.23 illustre la gestion des bits *a* et *b* (signalisation R2 ou Q.421) qui est une transposition numérique de la signalisation RON/TRON. La numérotation par impulsion (33/66) est transportée en émission par le bit « *a* », alors que la numérotation DTMF est acheminée en transparence sur le canal de voix.

Fonction	Emission		Réception	
	a	b	a	b
Repos	1	0	1	0
Prise de ligne	0	0	1	0
Invitation à numéroter	0	0	1	0
Impulsions de numérotation	0/1/0	0	1	1
Réponse	0	0	0	1
Raccrochage du demandé	0	0	1	1
Libération avant établissement	1	0	1	1
puis			0	1
Impulsions de taxation	0	0	0/1/0	

Figure 16.23 Gestion du bit a.

La signalisation par canal sémaphore sur lien numérique

La signalisation par canal sémaphore ou signalisation **CCS** (*Common Channel Signaling*) utilise un canal dédié (IT 24 de la trame T1, IT16 de la trame E1) pour signaler tous les événements relatifs aux communications établies sur la trame (signalisation, en mode messages, commune à tous les IT). Les protocoles utilisés sont des protocoles enrichis de type protocole D, CCITT N° 7 (SS7) ou propriétaire (l'IT est alors dépendante du constructeur).

La signalisation par canal sémaphore est adoptée par tous les constructeurs. Cependant, les PABX multiservices offrent aux utilisateurs des fonctionnalités plus riches que celles implémentées dans les protocoles de signalisation normalisés (figure 16.24).

Signalisation et réseau de PABX

Deux approches de la mise en relation de PABX sont à considérer. Dans la première, il s'agit simplement d'acheminer des communications téléphoniques sur des liens privés sans apport de téléservice aux utilisateurs (interconnexion de PABX). Dans la seconde approche, il s'agit non seulement d'acheminer les communications téléphoniques mais aussi les services associés (réseau de PABX). Dans ce dernier cas, l'ensemble des PABX du réseau est vu comme un seul PABX (PABX virtuel).

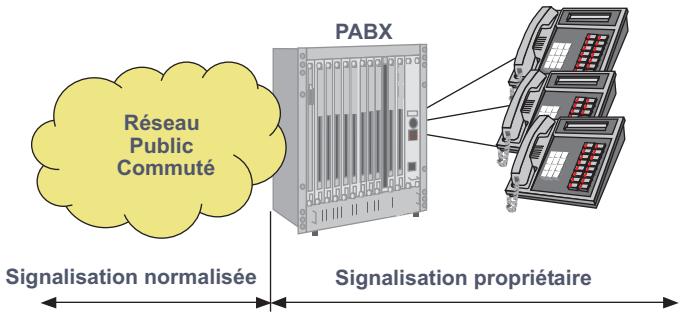


Figure 16.24 Le PABX et la signalisation.

➤ Interconnexion de PABX

Dans un réseau de PABX interconnectés, chaque PABX joue le rôle d'interface entre l'installation locale et le réseau privé d'une part et d'autre part entre l'installation locale et le réseau public. Lorsqu'un PABX est utilisé en tant que commutateur du réseau il est dénommé PABX de transit, il achemine alors les communications téléphoniques et la signalisation associée (figure 16.25).

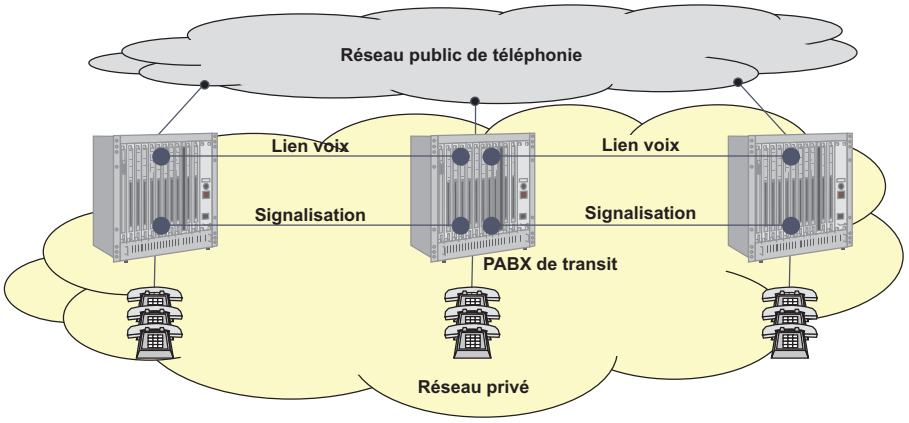


Figure 16.25 Interconnexion de PABX.

Pour des liaisons analogiques (LIA), la signalisation peut être transportée sur les fils de voix (LIA 2 fils) ou sur des fils séparés des fils voix (LIA 4 fils). Pour les liaisons numériques (MIC) un intervalle de temps, généralement l'IT16 peut être dédié au transport de la signalisation ou celle-ci peut être transportée par une liaison distincte. Chaque PABX de transit, interprétant la signalisation, peut éventuellement faire une conversion de celle-ci (arrivée sur un lien analogique et départ sur un lien numérique).

➤ Mise en réseau de PABX (Multisite)

La réalisation d'un multisite (ensemble du réseau vu comme un PABX virtuel) impose l'homogénéité de la signalisation sur l'ensemble du réseau. La figure 16.26 illustre le raccordement de trois PABX en réseau. Le lien d'interconnexion est un lien numérique structuré (MIC) avec ou sans IT16 selon les besoins de la signalisation du constructeur. Généralement, dans le cas

© Dunod – La photocopie non autorisée est un délit

d'une signalisation **CSS** (mode messages), l'IT16 peut être banalisé, la signalisation prise de ligne, numérotation et autres événements étant transportés par le canal sémaphore. Ce dernier peut être affecté à n'importe quel IT disponible ou à l'IT16.

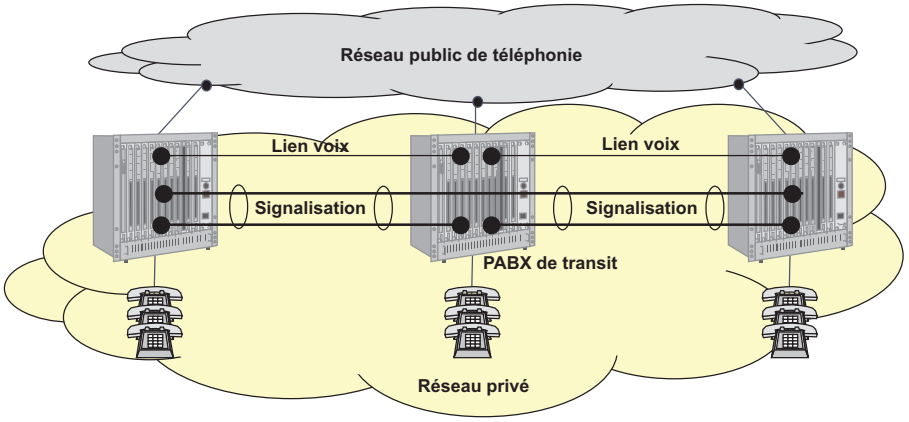


Figure 16.26 PABX en réseau et transport de la signalisation.

La différence essentielle entre un réseau de PABX interconnectés et un réseau de PABX (réseau dit aussi multisite) est dans le transport de la signalisation. L'ensemble des PABX étant vu comme un PABX virtuel un lien de signalisation en point à point doit être établi entre chaque PABX (réseau sémaphore). Ce lien pouvant être éventuellement dédié ou n'être qu'un circuit virtuel d'une liaison X.25. Le canal X.25 peut être séparé du lien voix (liaison LIA ou numérique) ou être transporté dans un IT d'une liaison numérique (MIC). L'utilisation de la signalisation SS7 simplifie le mode de diffusion de la signalisation, mais celle-ci devant être acheminée à travers le réseau nécessite qu'une fonction de commutation spécifique soit disponible dans les PABX (réseau de signalisation)

➤ Mise en réseau de PABX en milieu hétérogène

L'interconnexion de PABX hétérogènes se heurte à la non-homogénéité des protocoles de signalisation. La nécessité de disposer d'un protocole commun d'interconnexion a été résolue par le standard **DPNSS** (*Digital Private Network Signalling System*), très utilisé en Grande Bretagne mais non conforme au modèle OSI. Alcatel et Siemens, rejoints par l'ensemble des grands constructeurs, ont fondé le forum **IPNS** (*ISDN PABX Networking Specification*) destiné à définir un protocole commun d'interconnexion conforme au modèle OSI. Les travaux ont abouti à la normalisation (ECMA - ETSI - ISO) du protocole **Q-SIG** (*Signalisation au point Q*).

Q-SIG définit un point d'interconnexion (point Q) entre des réseaux hétérogènes. Ce n'est pas un protocole de bout en bout (usager à usager), chaque réseau reste sous le contrôle de son protocole propriétaire (figure 16.27).

Q-SIG, basé sur le protocole D (RNIS) dont il enrichit les messages, est orienté commutation de paquets en mode non connecté et connecté. Il ne définit que des services téléphoniques et non des fonctions de routage. Le transit (appel reçu par un PABX pour un usager raccordé à un autre PABX) est géré par le PABX sollicité en transit et non par le protocole d'interconnexion.

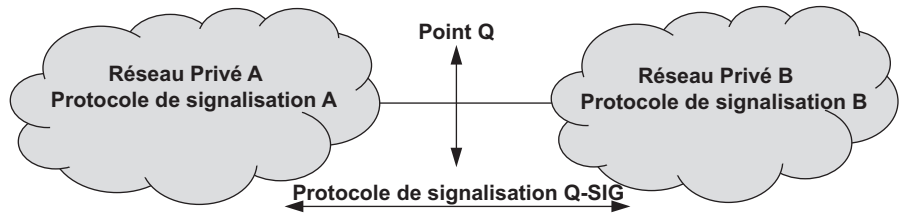


Figure 16.27 Position de la norme d'interconnexion Q-SIG.

Le tableau de la figure 16.28 compare les différentes fonctionnalités disponibles selon le protocole de signalisation utilisé.

Services	LIA	Transgroupe [8]	Q-SIG	Propriétaire
Facilités en émission				
Accès sélectif au réseau	•		•	•
Substitution				•
Num abrégée sur l'ensemble du réseau				•
Facilité en réception				
Acheminement par opératrice	•	•	•	•
SDA Euro-Numéris	•	•	•	•
SDA Transgroupe	•	•	•	•
Renvois à distance			•	•
Renvois en cascade	•	•	•	•
Filtrage				•
Interception d'appels				•
Protection contre l'interception				•
Outrepassement				•
Facilités en communication				
Va-et-Vient	•	•	•	•
Reprise d'appel	•	•	•	•
Conférence à trois	•	•	•	•
Transfert poste libre ou occupé	•	•	•	•
Transfert avec annonce	•	•	•	•
Parcage avec reprise du correspondant				•
Rappel automatique sur poste occupé			•	•
Rappel automatique sur poste libre			•	•
Rappel automatique sur faisceau occupé			•	•
Identification d'appels malveillants				•
Facilités propres au poste opérateur				
Intervention prioritaire			•	•
Outrepassement des renvois			•	•

8. La signalisation Transgroupe est la signalisation utilisée par France Télécom pour son offre de réseaux privés virtuels de téléphonie (Colisée Numéris).

© Dunod – La photocopie non autorisée est un délit

Services	LIA	Transgroupe	Q-SIG	Propriétaire
Outrepassement du non-dérangement			•	•
Affichage de l'état des terminaux (supervision)			•	•
Facilités des postes numériques				
Affichage date et heure				•
Identification correspondant intérieur		•	•	•
Dépôt de message (aviser)				•
Rappel du dernier appelant			•	•
Renvoi sur sonnerie (dévier)			•	•
Facilités système				
Changement de catégorie programmée				•
Faisceau de lignes extérieures	•		•	•
Débordement automatique	•		•	•
Renvoi général	•	•	•	•
Taxation au fil de l'eau			•	•
Taxation extérieure				•
Prépaiement				•
Dialogue avec l'autocommutateur				
Gestion de la numérotation abrégée				•
Gestion de la catégorie des postes				•
Gestion de la taxation				•
Annuaire				•

Figure 16.28 Comparaison des services disponibles selon la signalisation utilisée.

16.4 PRINCIPES DES RÉSEAUX VOIX/DONNÉES

16.4.1 Généralités

Le budget téléphonie représente plus de 80 % des dépenses de télécommunication (voix, données) des entreprises. Très tôt, il est apparu, qu'à partir d'un certain seuil de communication entre les divers établissements d'une entreprise, il devenait très avantageux de réaliser un réseau privé pour assurer le transport conjoint de la voix et de la donnée (partage de bande passante). L'échec de l'intégration des services de transport de données dans le PABX a conduit d'abord, à la réalisation de réseaux voix/données à l'aide de multiplexeurs (figure 16.29).

16.4.2 Les réseaux de multiplexeurs

Dans les réseaux de multiplexeurs temporels (TDM) les intervalles de temps sont affectés à un canal voix ou données (figure 16.31). De ce fait, lorsqu'une communication n'est pas établie la bande qui lui est allouée est perdue. Dans la trame multiplexée représentée figure 16.30, les canaux 3 à 5, n'ayant aucunes données à transmettre, sont inutilisés, la bande est perdue.

L'avantage des multiplexeurs temporels réside essentiellement dans la simplicité des algorithmes de gestion, ce qui autorise des temps de traitement courts et donc des délais de transit dans le réseau faibles.

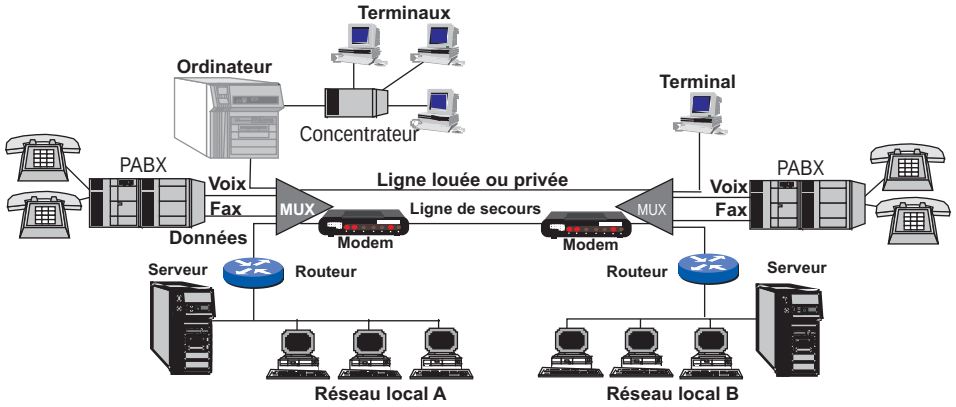


Figure 16.29 Principe des réseaux voix/données.

Le TDM n'est pas une technique adaptée aux transferts de données sporadiques comme en provoque l'interconnexion des réseaux locaux. Ces inconvénients sont résolus par l'utilisation de multiplexeurs statistiques mais d'un coût plus élevé.

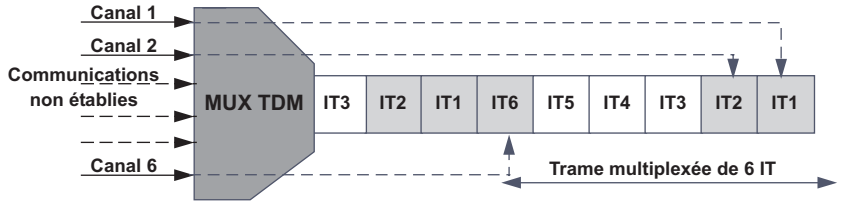


Figure 16.30 Principe de l'allocation statique des canaux dans un MUX TDM.

16.4.3 La voix paquetisée

Généralités

Plusieurs raisons conduisent à transmettre la voix sur des systèmes à commutation de paquets :

– dans une infrastructure d'interconnexion de PABX, les canaux voix ne sont pas utilisés en permanence ;
– le caractère *half-duplex* d'une conversation et les temps de silence qui entrecoupent la conversation permettent de récupérer jusqu'à 60 % de la bande allouée à une communication téléphonique.

Pour cela, il convient de modéliser le flux voix comme un flux de données en transformant le flux d'information constant (échantillons) en un flux périodique (paquets). Si on peut garantir aux paquets, un transfert respectant les contraintes temporelles du transfert isochrone, il est alors possible d'utiliser un réseau à commutation de paquets pour transmettre la voix. Le multiplexage par étiquette, utilisé par la commutation de paquets, garantit une utilisation optimale de la bande (figure 16.31), une administration unifiée du réseau, une réduction des coûts (la voix étant transportée selon la tarification de la donnée, généralement forfaitaire) et la suppres-

© Dunod – La photocopie non autorisée est un délit

sion des coûts de l'infrastructure téléphonique si l'entreprise disposait d'un réseau voix et d'un réseau données séparés.

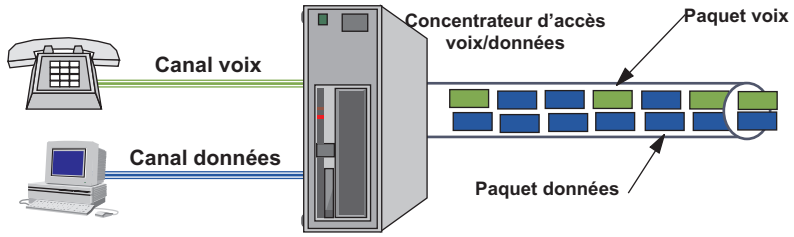


Figure 16.31 Paquetisation de la voix et réseau à commutation de paquets.

Pour garantir le transport de la voix, les systèmes d'interconnexion de réseaux voix/données doivent assurer :

- un débit minimal garanti, les flux voix ne devant jamais occuper plus de 50 % de la bande passante du support ;
- un transfert dans un délai aussi réduit que possible par prioritisation des flux voix (< 150 ms, avec une tolérance jusqu'à 200 ms) ;
- la maîtrise de la gigue dans le réseau et en assurer la correction dans la passerelle destination ;
- la reprise sur erreur n'ayant aucun sens pour les flux temps réel et malgré une faible sensibilité de la voix aux erreurs, un transfert correct de la voix nécessite un taux d'erreur relativement faible ;
- pour garantir une utilisation optimale de la bande passante, un système de détection des silences doit être implémenté (**DSI**, *Digital Speech Interpolation*). Pour ne pas perturber l'interlocuteur distant, durant la récupération de bande (détection et récupération des temps de silence), il convient, localement, de restituer un bruit de fond. À cet effet des paquets spécialisés (paquets de silence) seront émis par la source.

Techniques mises en œuvre dans les réseaux voix/données

➤ Compression de la voix

Afin d'optimiser l'utilisation de la bande passante, les techniques de compression de voix sont implémentées dans tous les systèmes voix/données. Ces techniques apportent une réduction importante de la bande utilisée en contrepartie d'un temps de traitement non négligeable.

La voix analogique est numérisée et codée par le PABX (**MIC** ou **PCM** *Pulse Code Modulation*, norme G.711 à 64 kbit/s), l'équipement d'interconnexion effectue ensuite la compression (figure 16.32). Les techniques utilisées sont spécifiques, il ne s'agit pas réellement de compression des données voix, mais d'un codage spécifique réducteur de bande.

La méthode la plus simple, et donc la plus économique est **l'ADPCM** (*Adaptive Differential Pulse Code Modulation*, norme G.726). L'ADPCM réalise un codage différentiel par comparaison de la valeur de chaque échantillon à la valeur de l'échantillon précédent. Le sens de la variation est codé sur un bit, l'amplitude sur 1, 2 ou 3 bits, ce qui correspond respectivement à

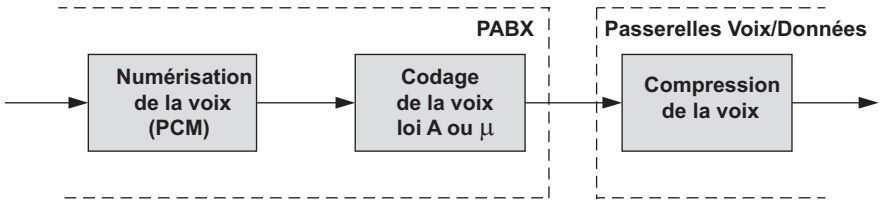


Figure 16.32 Principe de la compression de voix.

des débits de 16, 24 ou 32 kbit/s. Indépendamment de la réduction de bande l'ADPCM est plus résistant aux erreurs que le codage MIC. Cependant, cette technique est aujourd'hui obsolète.

Des techniques plus élaborées s'appuient sur les caractéristiques du spectre de fréquence de la parole. Ces systèmes analysent (2,5 à 30 ms, selon le système) la voix et réalisent une prédiction linéaire du signal de voix à partir des quatre derniers échantillons (vecteur). Ils comparent le vecteur obtenu à une table de vecteurs préétablie, seul l'index d'entrée dans la table et une information d'amplitude sont envoyés au récepteur. Ce dernier reconstitue le signal d'origine à partir du vecteur et d'une série de filtres modélisant le conduit vocal de l'interlocuteur. Les codeurs **CELP** (*Code Excited Linear Predictive*) sont particulièrement performants. Ils n'introduisent qu'un faible retard dû à l'acquisition des données et à la prédiction (prétraitement de la trame suivante ou *look ahead*). Plusieurs variantes existent. Le tableau de la figure 16.33 présente les différents systèmes et leurs caractéristiques. La qualité de restitution est exprimée en **MOS** (*Mean Opinion Score*). Cette notation réalisée par un groupe de personne sur l'écoute de plusieurs échantillons de voix est toute subjective.

Normes	Appellation	Débit (kbit/s)	Retard (ms)	MOS	Calcul (MIPS)	Trame (octets)
G.711	PCM	64	0,125	4,1	0,34	1
G726	ADPCM	32, 24, 16	0,300	3,85	14	
G.723.1	MP-MLQ	6,3	90	3,9	16	24
G.723.1	ACELP	5,3	90	3,9	16	20
G.728	LD-CELP	16	3	3,9	33	
G.729	CS-ACLEP	8	30	3.92	20	10
G.729a	CS-ACLEP	8	30	3,7	10,4	10

Le retard indiqué comprend le temps de codage et de décodage
MP-MLQ *Multiple Pulse Maximum Likelihood Quantizer*
LD-CELP *Low Delay CELP*
CS-ACELP *Conjugate Structure Algebric CELP*

Figure 16.33 Synthèse des systèmes de compression de voix.

Les normes G.72x ne traitent pas les silences (sauf G.729b). Durant les silences un signal réduit est transmis. Les normes G.729a et G.723.1 (ACLEP) sont les plus utilisées d'une part par la qualité du son restitué et d'autre part par la faible puissance de calcul nécessaire (**MIPS**, Million d'Instructions Par Seconde). D'autres techniques autorisent des réductions de bande plus importantes. Toutefois, au-dessous de 8 kbit/s la qualité de restitution est généralement insuffisante. Ces techniques, souvent propriétaires, imposent une homogénéité des équipements sur l'ensemble du réseau.

© Dunod – La photocopie non autorisée est un délit

Dans un réseau voix/données deux modes d'établissement des communications sont envisageables. Le premier, le plus simple consiste à transporter la signalisation de manière transparente. Les informations de signalisation ne sont alors pas interprétées par les passerelles voix/données et sont acheminées comme de simples données. Le routage des communications est alors réalisé par les PABX dit PABX de transit. Cette opération conduit à une décompression et à une recompression de la voix. Indépendamment des délais introduits, ce mode d'établissement des communications (figure 16.34) par les opérations de compression et de décompression altère fortement la qualité de la voix et limite le nombre de bonds dans le réseau.

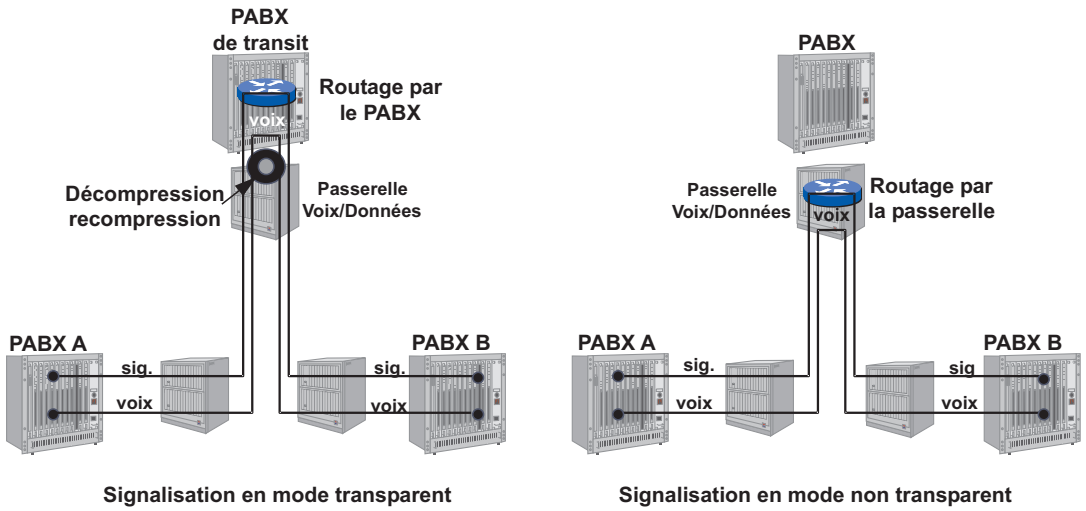


Figure 16.34 Communication entre les PABX A et B.

Dans le deuxième mode, dit non transparent, l'acheminement de la communication est réalisé par les passerelles voix/données qui interprètent la signalisation et assurent alors le routage de la communication. Le signal de voix n'a pas à être décompressé et recompressé. L'élongation du réseau n'est alors limitée que par les temps de transfert et de traitement.

➤ Limitation et correction de la gigue

Le temps total de transfert ou temps de bouche à oreille intervient dans l'interactivité de la communication téléphonique, alors que la variation de ce temps ou gigue est un processus réducteur de la qualité auditive de la communication. La gigue dans un réseau voix/données a deux origines. La première est liée aux délais variables de traitements des données par chaque élément du réseau, elle dépend de la charge de celui-ci et du dimensionnement du réseau (files d'attente). La seconde est liée directement à la nature des flux. Compte tenu de la spécificité des différents flux, dans les équipements voix/données les flux voix et données sont séparés et mis, en attente de traitement, dans des files d'attente différentes. Le traitement de la voix bénéficie d'une priorité absolue, tant qu'un paquet voix est présent, la file d'attente données est bloquée. Ce n'est qu'en l'absence de voix, ou entre 2 paquets voix que les paquets données sont traités et émis. La figure 16.35 illustre ce mécanisme. Les paquets de voix sont émis avec une période de récurrence constante (flux isochrone), cependant l'insertion d'un paquet

de données engendre un retard dans l'émission du paquet voix suivant. Ce retard dépend de l'instant d'arrivée du paquet voix et de sa taille.

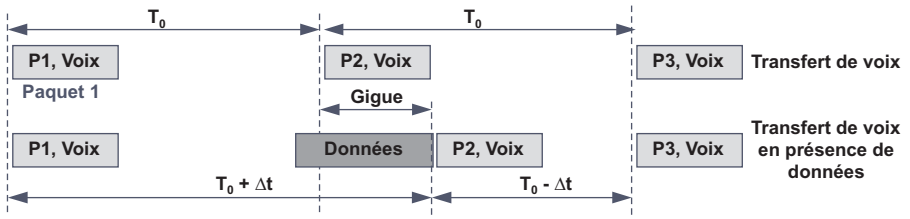


Figure 16.35 Introduction d'une gigue par l'émission d'un paquet voix.

Pour limiter la gigue, les paquets de données devront être aussi petits que possible (fragmentation des paquets de données en présence de paquets voix). Chaque nœud intermédiaire franchi introduit, en présence de données, une variation de délai de transit. La gigue totale résulte de la somme des variations de délai introduits par chacun des nœuds. En sortie du réseau, la passerelle voix/données doit insérer un buffer « élastique » pour corriger cette gigue (figure 16.36). Si le buffer de gigue résout le problème de variation des délais, il allonge le temps de transfert de bout en bout.

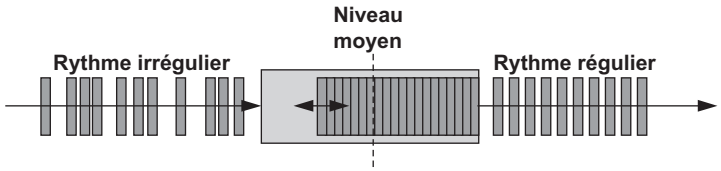


Figure 16.36 Principe de la correction de gigue par buffer « élastique ».

➤ Traitement des télécopies

La voix, même dégradée en qualité, est reconnaissable, il n'en est pas de même des données de télécopie. La solution généralement adoptée consiste à reconnaître les modulations, détecter la porteuse (exemple pour le V.29 porteuse à 2 100 Hz), la démoduler et transmettre les données numériques issues du Fax comme une donnée ordinaire. Le système récepteur opérera à l'inverse en remodulant avant de remettre le signal au PABX destinataire.

➤ Traitement de l'écho

Le poste de l'usager est raccordé par deux fils (boucle locale), la liaison distante comporte généralement quatre fils (paire émission et paire réception). Un transformateur différentiel assure le passage de deux à quatre fils. Si l'adaptation d'impédance est mal réalisée, une partie de l'énergie est réfléchie : c'est l'écho. Les différents types d'écho sont représentés figure 16.37.

L'écho local est peu gênant. À partir d'un certain délai de transmission, fonction de la distance séparant les deux PABX, l'écho distant peut devenir gênant. Supérieur à 45 ms, il constitue un véritable trouble de la conversation[9].

9. L'IUT limite à 24 ms le temps de propagation dans un réseau. Au-delà, l'emploi d'annulateur d'écho est obligatoire.

© Dunod – La photocopie non autorisée est un délit

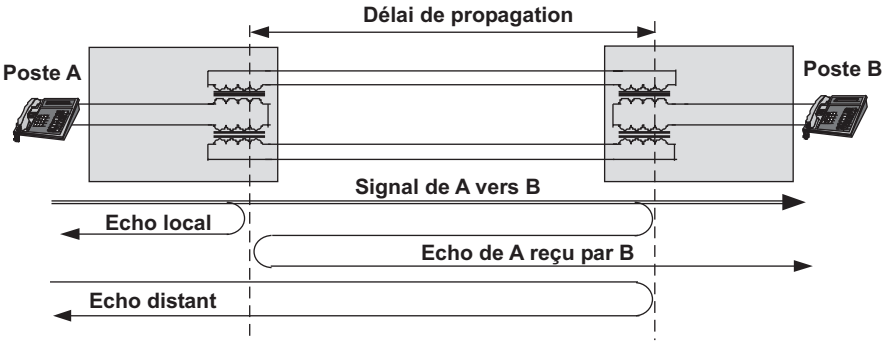


Figure 16.37 L'écho dans une liaison téléphonique.

S'il ne peut être évité, il convient de l'éliminer, les annulateurs d'écho effectuent cette fonction. Les annulateurs d'écho[10] construisent un modèle mathématique de la voix sur une voie, et réinjectent ce signal en opposition sur l'autre voie. Le principe des annulateurs d'écho est illustré figure 16.38. L'installation doit être symétrique (2 annuleurs d'écho par liaison).

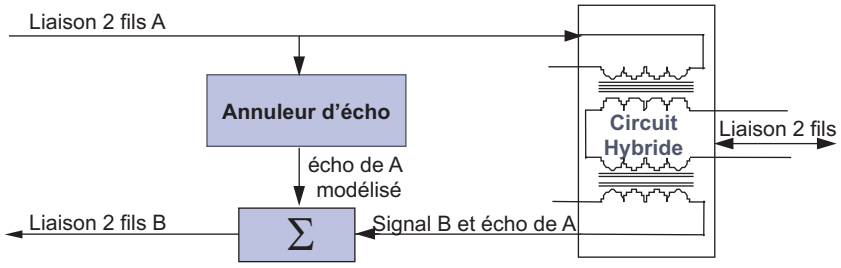


Figure 16.38 Principe des annulateurs d'écho.

➤ Traitement des silences

Lors d'une conversation seule une personne parle, son ou ses interlocuteurs écoutent et sont donc silencieux. Durant ces silences, le seul signal présent correspond aux bruits d'ambiance. Le signal de parole pouvant être modélisé (niveaux de puissance, spectre de fréquence), il est alors possible de détecter les silences et de ne rien transmettre durant ces instants. Cependant, l'absence de bruit chez le correspondant distant peut lui faire croire que son interlocuteur a raccroché. Pour éviter ceci et recréer l'ambiance d'une communication téléphonique classique, des paquets spécifiques peuvent alors être émis pour signaler au système destinataire le silence. Celui-ci génère alors un bruit de fond. La bande passante récupérée peut atteindre 60 % de la bande nominale.

La figure 16.40 illustre le traitement des silences. Après l'étape de numérisation classique (G.711), la voix est analysée pour calculer le signal d'annulation d'écho (G.165/G.168). Afin de récupérer de la bande passante, le système de traitement des silences ou **VAD** (*Voice Activity*

10. Précédemment les réseaux utilisaient des suppresseurs d'écho, ces systèmes plus simples interdisaient la transmission full duplex. Lors de telle transmission, il fallait inhiber la suppression d'écho par l'émission d'un signal de commande à 2 100 Hz.

detection) détecte les silences, la voix est ensuite compressée. Enfin, l'ensemble des informations est mis en paquets (paquets de voix ou paquets de silence). Les paquets de silence ne transportent aucune donnée, ils ne sont utilisés que pour signaler une absence de paquets voix, et non une perte, et permettre au destinataire de générer un bruit aléatoire de fond.

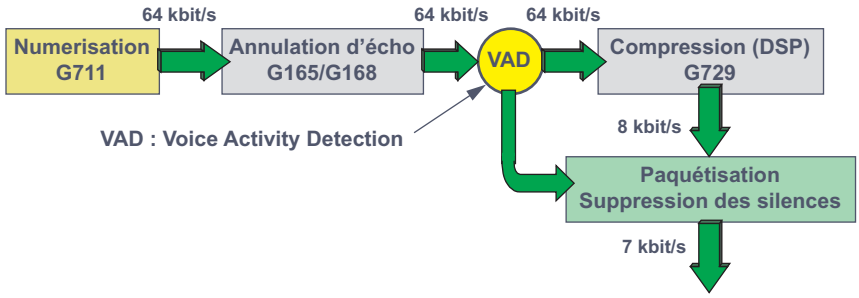


Figure 16.39 Exemple de système de traitement des silences.

Dans l'exemple de la figure 16.39, le débit minimal d'environ 7 kbit/s correspond au débit de ligne après les diverses encapsulations du signal. Lors du dimensionnement d'un système voix/données, il ne faut pas tenir compte de cette récupération de bande pour définir les canaux voix, ils doivent l'être au maximum de la bande requise, soit dans notre exemple 17,8 kbit/s (encapsulation RTP/UDP/IP/PPP, voir section 16.7, voix sur IP).

Modes de relation téléphonique dans les réseaux paquets

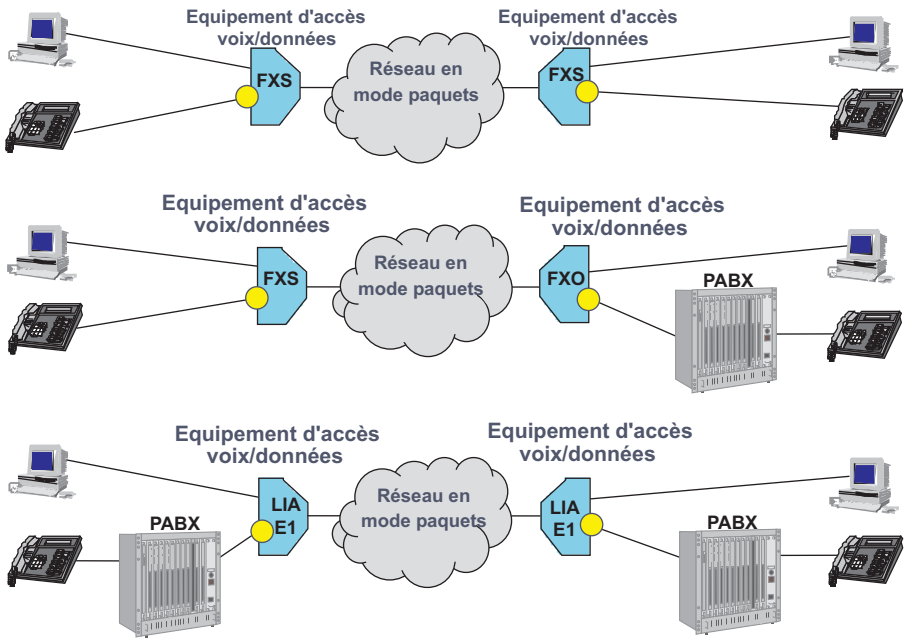


Figure 16.40 Mode de mise en relation à travers un réseau en mode paquets.

© Dunod – La photocopie non autorisée est un délit

Trois modes de mise en relation téléphonique peuvent être distingués (figure 16.40). Un réseau voix/données peut mixer ces différentes configurations :

– le mode « postes de service » met en relation directe deux ou plusieurs postes téléphoniques analogiques isolés utilisant la signalisation RON/TRON. L'interface **FXS** (*Foreing eXange Station*) émule vis-à-vis du poste téléphonique un PABX ;

– le mode « postes déportés » permet de relier un ou plusieurs postes analogiques distants (signalisation RON/TRON) à travers une interface **FXO** (*Foreing eXchange Office*) et FXS à un PABX. Les postes distants ont accès aux postes de l'installation locale, et réciproquement. Ils ont aussi accès, via le PABX, au réseau téléphonique public. L'interface FXO émule vis-à-vis du PABX un ou plusieurs postes téléphoniques ;

– le mode « interconnexion de PBX » vise à la réalisation de réseaux privés de téléphonie, il utilise des interfaces de type LIA ou E1. Outre la voix, ce système assure le transfert de la signalisation téléphonique (RON/TRON, Q.931, MF Socotel, Colisée, QSig...).

16.5 LA VOIX SUR ATM

Initialement prévu pour assurer l'évolution du réseau RNIS vers le large bande, ATM assure de manière native le transport de la voix au-dessus de l'AAL1 (service **CBR**, *Constant Bit Rate*). Pour optimiser l'utilisation de la bande passante, l'ATM Forum a spécifié deux modes d'utilisation de l'ATM pour réaliser des réseaux voix (figure 16.41), le mode CES et le mode VTA.

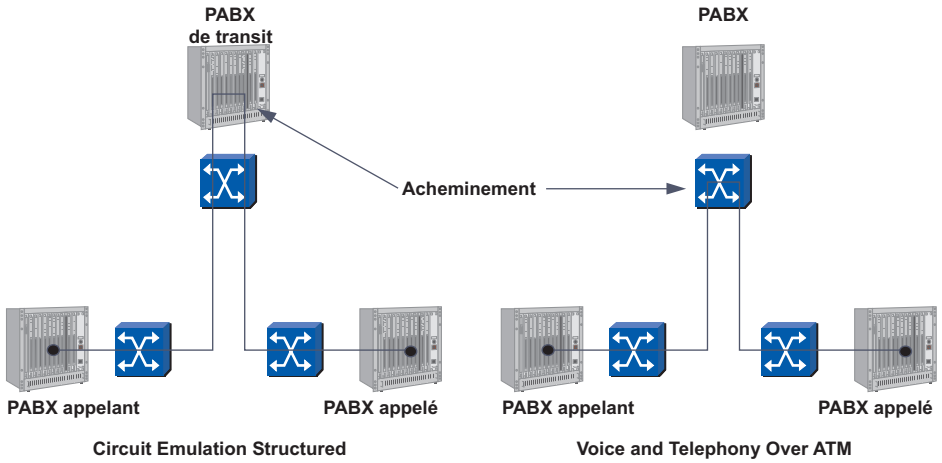


Figure 16.41 La voix dans les réseaux ATM.

Le mode **CES** (*Circuit Emulation Structured*) permet l'interconnexion de PABX via un réseau ATM. La signalisation est transportée en mode transparent : elle est interprétée par les PABX qui effectuent le routage des communications, ces PABX sont dits : PABX de transit. Assis sur l'AAL1, le CES procède par réservation de bande, il n'exploite pas les possibilités d'ATM, et ne permet pas une gestion dynamique de la bande passante. Le CES est comparable au multiplexage temporel.

Le PABX est relié au commutateur via une interface E1 en mode structuré (G.703/G.704, lien de *n* fois 64 kbit/s). Le service est du type circuit virtuel permanent (PVC, *Permanent Virtual Circuit*). Chaque liaison ne nécessite qu'un PVC pour la voix (multiplexage des communications sur le PVC) et un PVC entre chaque PABX raccordé pour la signalisation (maillage complet). Entre le PABX et le commutateur d'accès, la signalisation du PABX peut être transportée dans l'IT16 de l'interface E1 (E1 structuré) ou utiliser un canal dédié (généralement du type X.25 ou simple lien HDLC).

Dans le mode **VTOA** (*Voice and Telephony Over ATM*) la signalisation est transportée en mode non transparent. VTOA ne privilégie pas une AAL particulière, seul un service de type VBR-rt (*Variable Bit Rate real time*) est requis. Le lien entre le commutateur de rattachement et le PABX est du type E1 structuré, la signalisation du type canal sémaphore (signalisation dite **CCS**, *Common Channel Signaling*) utilise le canal 16 ou un lien dédié (PVC). Les liaisons voix peuvent utiliser des liens de type **PVC** ou **SVC** (*Switched Virtual Circuit*). La signalisation peut être du type SS7, Q.931, QSIG, DPNSS... Elle est directement interprétée par les commutateurs qui effectuent le routage des communications, un seul lien de signalisation est alors nécessaire.

La figure 16.42 compare succinctement les deux solutions de la voix sur ATM.

Critères	CES	VTOA
Type de service	CBR	VBR-rt
Optimisation de la bande	Transport de nature TDM	Allocation dynamique de la bande
Signalisation	En mode transparent	Interprétation de la signalisation
Routage des communications	PABX de transit	Commutateurs du réseau
Types de liens	PVC uniquement	PVC et SVC

Figure 16.42 Comparaison de VTOA et du CES.

16.6 LA VOIX ET LE FRAME RELAY

Face aux lenteurs de la normalisation d'ATM et à une relative complexité de l'administration d'un réseau ATM, les réseaux privés Frame Relay se sont rapidement imposés comme l'évolution naturelle des réseaux X.25. Le besoin de rentabiliser les liens a rapidement conduit certains constructeurs à implémenter dans les FRAD (*Frame Relay Access Device*) des fonctionnalités de transfert de voix sur le Frame Relay (**VFRAD**, *Voice FRAD*). La figure 16.43 illustre un réseau voix sur Frame Relay. Le réseau Frame Relay pouvant être privé ou public. Face à ces développements et bien que le Frame Relay ne soit pas prévu pour le transfert des flux isochrones, le Frame Relay Forum a défini le transport de la voix sur Frame Relay dans sa recommandation FRF11 et le transfert de données en présence de voix (trames de données de longueur fixe) dans la FRF12 (segmentation). Ces recommandations définissent les services voix, télécopie, modem analogique, données et le multiplexage de ces différents flux.

La recommandation FRF11 (**VoFR**, *Voice over Frame Relay*) spécifie :

– le multiplexage de canaux voix et données sur le même DLCI (*Data Link Circuit Identifier*). Cette possibilité ne sera utilisée que sur un réseau public tarifé au DLCI. Sur un réseau privé on séparera les flux pour améliorer la qualité de service ;

© Dunod – La photocopie non autorisée est un délit

– le multiplexage de plusieurs canaux voix sur le même DLCI (jusqu'à 255) ;
– le regroupement de plusieurs canaux voix dans une seule trame (concaténation) ;
– le support de différents algorithmes de compression (G.711 ; G.726 à 40, 32 et 16 kbit/s ; G.727, G.728 et G.729) ;
– la signalisation ;
– la gestion des priorités ;
– l'utilisation de connexion Frame Relay à faible débit (classe 2) ou à débit élevé (classe 1). Les algorithmes de compression associés diffèrent selon la classe du réseau.

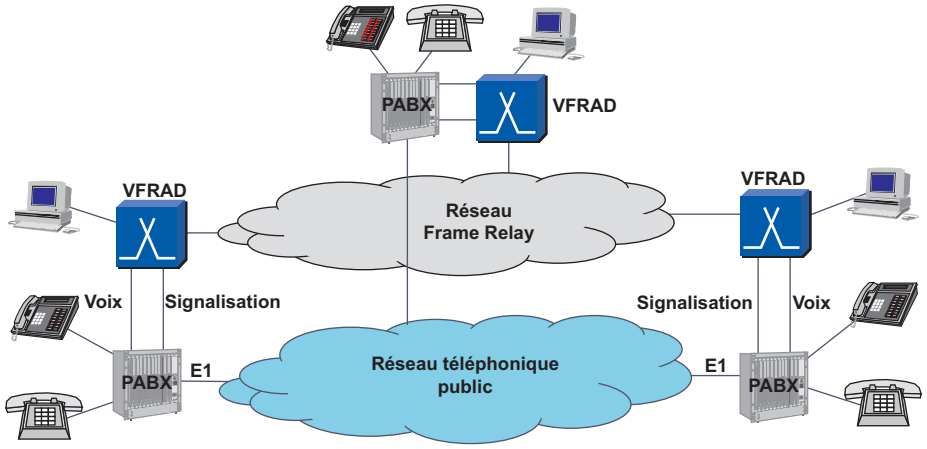


Figure 16.43 Architecture générale d'un réseau voix/données Frame Relay.

Pour permettre le multiplexage de plusieurs canaux voix (communications) et de la donnée sur un même DLCI, la FRF11 définit une encapsulation supplémentaire (sous-trame ou *sub-frame*) représentée figure 16.44.

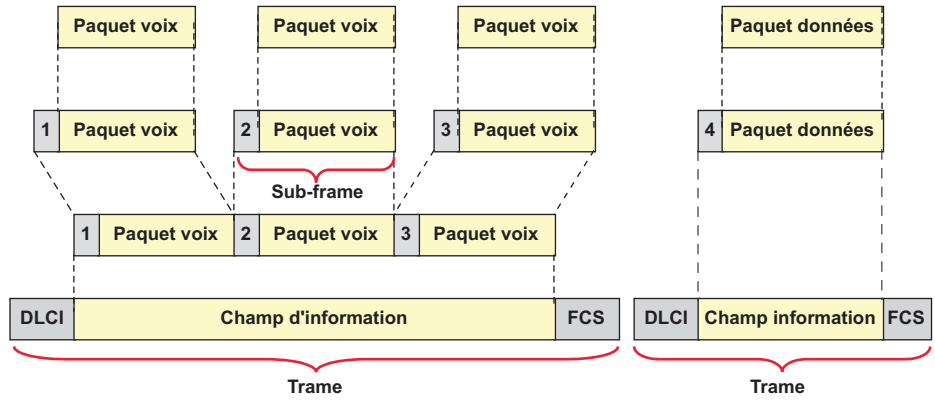


Figure 16.44 Multiplexage des canaux dans une même trame Frame Relay.

La figure 16.45 présente le format de l'en-tête des sous-trames. L'en-tête a un format variable selon que la sous-trame est seule ou la dernière d'une trame (bit LI = 0).

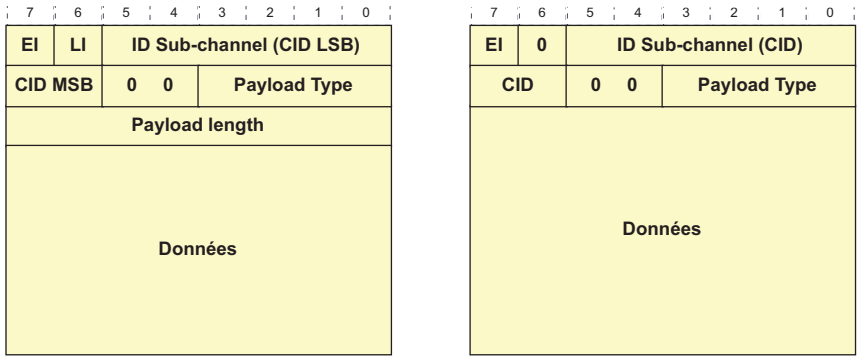

7 6 5 4 3 2 1 0
EI LI ID Sub-channel (CID LSB)
CID MSB 0 0 Payload Type
Payload length
Données
7 6 5 4 3 2 1 0
EI 0 ID Sub-channel (CID)
CID 0 0 Payload Type
Données

Figure 16.45 VoFr, en-tête des sous-trames.

Le bit **EI** (*Extended Indicator*) précise la longueur du champ **CID** (*Channel Identification*), à 0 les canaux sont identifiés sur 6 bits (64 canaux dans un même DLCI) ou 8 bits (255 canaux). Le champ **LI** (*Length Indicator*) indique si le champ longueur des données (*Payload length*) est présent ou pas. Il est à 0 si la sous-trame est la seule transportée ou est la dernière de la trame. Il est à 1 dans toutes les autres sous-trames. Le champ *Playload Type* indique le type de données transportées (voix, données, fax, bits de signalisation CAS). Le bit EI à 0 indique que la charge utile est de la voix codée en EADPCM (G.727) pour les réseaux de classe 1 ou de la voix CS-ACLEP (G.729) pour les réseaux de classe 2. Dans ce dernier cas l'octet *Payload Type* n'est pas présent.

La recommandation FRF11 autorise aussi le regroupement ou *Packing Factor* de plusieurs paquets voix d'une même communication dans une même sous-trame. Cette pratique améliore le rendement du protocole (réduction de *l'overhead*) mais allonge les délais et rend le transfert plus sensible aux erreurs.

Le Frame Relay est une excellente solution au transport de la voix et des données sur des réseaux privés ou publics à faible ou moyen débit. Cependant, l'apparition de la voix sur IP a réduit le Frame Relay à n'être plus que la couche liaison d'un réseau IP transportant la voix sur IP.

16.7 LA VOIX ET TÉLÉPHONIE SUR IP

16.7.1 Généralités

Deux approches de la voix sur IP doivent être distinguées (figure 16.46). La première, à l'instar d'ATM et du Frame Relay consiste à transporter la voix traditionnelle sur un réseau IP, nous l'appellerons voix sur IP (**VoIP**, *Voice over IP*). La seconde utilise le protocole IP de bout en bout, les téléphones (IP phone) sont directement connectés à un LAN IP, c'est la téléphonie sur IP (**ToIP**, *Telephony over IP*).

S'appuyant sur une technologie en mode non connecté, la voix sur IP nécessite l'utilisation de protocoles complémentaires pour le transport de données temps réel afin d'assurer la resynchronisation des paquets, de garantir la priorité des flux multimédia et la gestion de la congestion du réseau. Ces protocoles sont essentiellement :

© Dunod – La photocopie non autorisée est un délit

– **RTP** (*Real Time Protocol*, RFC 1889 et RFC 1890) qui assure l'horodatage et le contrôle de séquencement des paquets ;
– **RSVP** (*Resource reSerVation Protocol* de l'IETF, Q.397 de l'UIT) qui autorise, pour les flux multimédias, une réservation de ressources réseau de bout en bout. Ce protocole permet la cohabitation de flux multimédia et de flux sporadiques non prioritaires ;
– **MPPP** (*Multilink PPP*, extension de la RFC 1717) qui assure la segmentation des paquets de données longs (*jumbogram*) en petits paquets et autorise le multiplexage de ces paquets avec des paquets temps réel (*Multilink fragmentation and interleaving*).

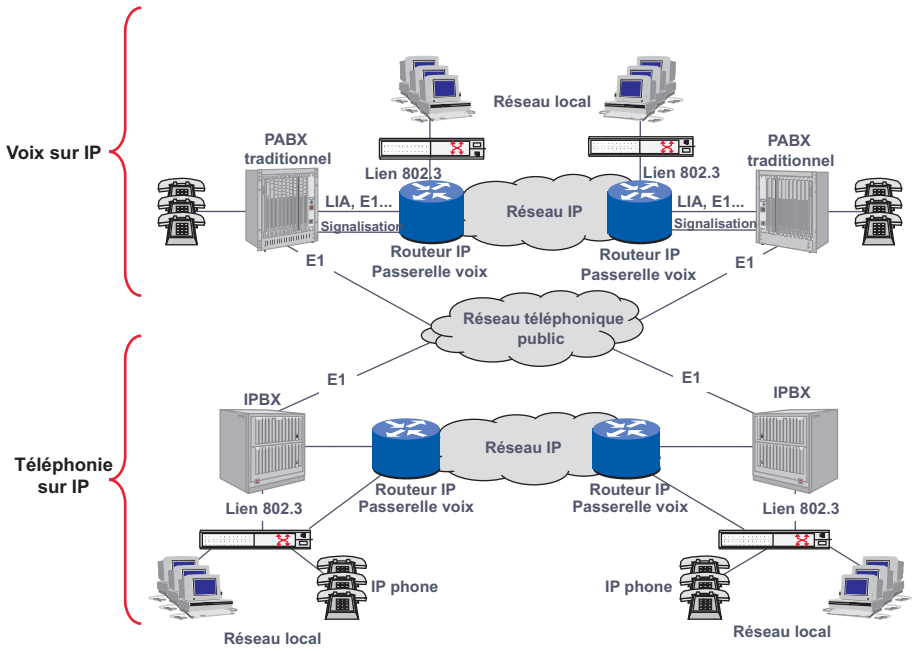


Figure 16.46 Voix sur IP.

L'ensemble s'intégrant dans un modèle architectural décrit par l'UIT, le modèle H.323. Ce modèle permet l'établissement de communication entre terminaux IP/IP (IP phone) et des terminaux IP/Traditionnel. H.323 détermine les protocoles de signalisation interne au réseau et assure la conversion de signalisation vers les réseaux publics.

16.7.2 TCP/IP et le temps réel

Pour des raisons d'efficacité le protocole **UDP** (*User Datagram Protocol*) s'impose pour le transfert des flux multimédia :

– pas d'ouverture, ni de fermeture de session ;
– pas d'acquittement, ni de reprise sur erreur ;
– pas de contrôle de flux et de congestion ;
– faible temps de latence.

Deux protocoles complémentaires ont été adjoints à UDP, le premier **RTP** (*Real Time Protocol*) a essentiellement pour objet de fournir les informations nécessaires à la correction de gigue. Le second, intégré dans RTP, **RTCP** (*Real Time Control Protocol*) fournit périodiquement des informations sur la qualité du réseau. La figure 16.47 illustre les différents flux protocolaires.

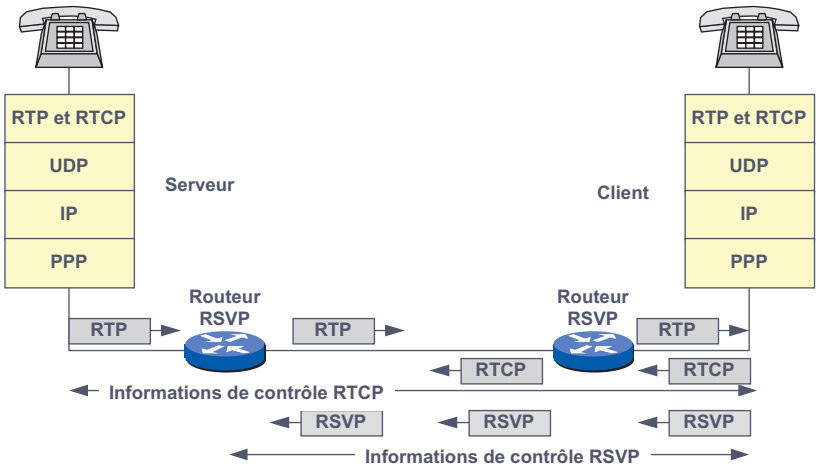


Figure 16.47 Le contrôle de session par RTP et RTCP.

Dans une session multimédia, chaque flux est transporté par une session RTP distincte. De même, à chaque session RTP est associé un flux de contrôle RTCP. Une session RTP est une association de plusieurs communicants, au moins 2, une session est identifiée par le couple port/adresse. L'en-tête RTC contient les informations d'identification, de séquencement, de type de charge utile et d'horodatage (figure 16.48).

Ver	P	X	CC	M	PT (type de charge)	Numéro de séquence
RTP Time Stamp						
Identifiant de la source de synchronisation (SSRC)						
Identifiant des flux (CSRC)						

Figure 16.48 En-tête RTP.

Sur 2 bits, le champ Ver indique la version de RTP (actuellement 2). Le bit P indique s'il y a (1) ou non (0) des octets de bourrage. Le nombre d'octets de bourrage est précisé dans la charge utile. Le X précise s'il y a des extensions d'en-tête. Le bit M (*Marker*) définit un profil RTP, par exemple, si la récupération des silences est activée, dans chaque premier paquet d'un échange ce bit est à 1. Le champ PT (*Payload Type*) indique le type de charge utile et le format de codage. Le numéro de séquence est incrémenté de 1 à chaque paquet, le numéro de séquence initial est aléatoire. Le champ *Time Stamp* indique sur 32 bits l'instant d'échantillonnage du premier octet du paquet RTP. Cette information permet la récupération de la gigue, sa valeur initiale est aléatoire. Le champ SSRC (*Synchronisation Source Report Count*), unique au sein d'une session RTP, identifie la source sur laquelle les paquets de données sont synchronisés. Le champ CSRC (*Contributing Source*) est utilisé quand plusieurs sources fournissent des

© Dunod – La photocopie non autorisée est un délit

informations et que le paquet contient des informations reconstituées à partir de ces différentes sources.

L'encapsulation IP/UDP/RTP ajoute 20 octets au paquet de données, sans compter l'en-tête de niveau 2. Le tableau de la figure 16.49 indique la bande passante, arrondie au kbit/s le plus proche, requise en fonction du type de protocole de niveau 2.

Algorithme	Débit Codec kbit/s	Charge utile/ Nb paquets seconde	Niveau 3	Niveau 2			
			IP/UDP/RTP	Ethernet	PPP	Frame Relay	ATM
Octets overhead			40	26	6	6	5
G.711	64	160/50	80	90	82	82	88
G.711	64	240/33	74	81	76	76	84
G.723.1	6,3	24/33	17	24	18	18	28
G.729	8	20/50	24	34	26	26	42

Figure 16.49 Bande utile après encapsulation.

Le rapport charge utile/données de service est tel qu'un mécanisme de compression d'en-tête (**CRTP**, *Compressed Real Time Transport Protocol*, RFC 1144), basé sur la redondance des informations d'en-tête permet de réduire d'un facteur d'environ 10 (en-tête de 2 à 4 octets) la taille des données de service (figure 16.50). Par exemple, la compression CRPT associée à la récupération des silences réduit le débit du G.723.1 de 18 à 6 kbit/s. La compression CRTP compresse les données lien par lien, ce qui signifie d'une part que tous les équipements intermédiaires doivent supporter la compression CRTP et d'autre part que ce traitement induit un délai supplémentaire d'autant plus important que le nombre de bonds l'est.

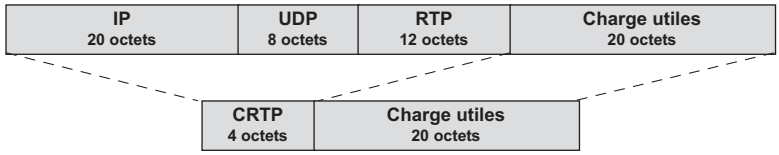


Figure 16.50 Compression d'en-tête CRTP.

Pour limiter la gigue, le protocole **MLPPP** (*MultiLink PPP*, RFC 1144) fragmente les paquets longs. Les petits paquets, notamment ceux de voix, sont encapsulés normalement et entrelacés (multiplexés) avec le flux fragmenté (figure 16.51).

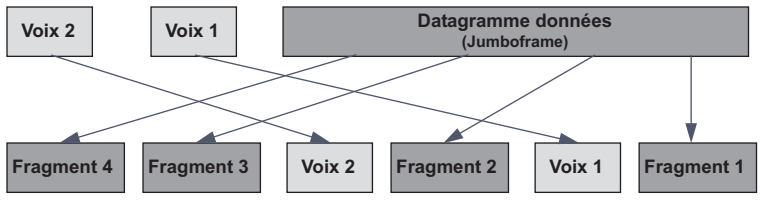


Figure 16.51 Entrelacement des paquets voix et données (MLPPP).

16.7.3 L'architecture H.323 de l'UIT

La recommandation H.323 définit un modèle architectural pour assurer le transport de la voix sur un réseau en mode paquets de type IP, c'est-à-dire sans qualité de service. L'architecture H.323 comprend diverses fonctionnalités (ou éléments) représentées figure 16.52.

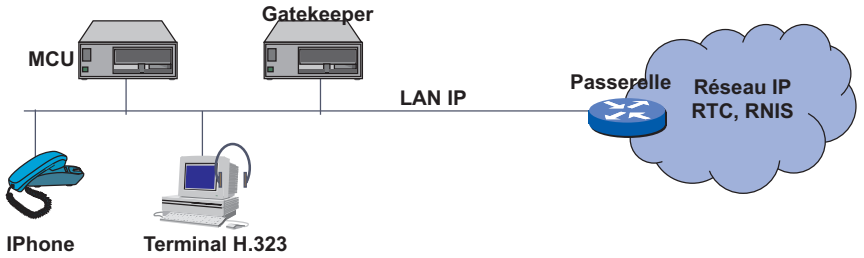


Figure 16.52 Architecture matérielle d'une zone H.323.

Les terminaux H.323 sont raccordés directement au LAN IP. Ils ont la capacité d'établir des communications voix, vidéo et/ou données en temps réel avec tout terminal de la zone H.323 ou non en mode point à point, multipoint ou diffusion. L'appel est réalisé selon le protocole Q.931 (protocole D du RNIS). Les protocoles mis en œuvre par un terminal H.323 sont :

– H.225 ou **RAS** (*Registration Admission Status*), ce protocole gère l'enregistrement auprès d'une passerelle (*Registration*), réalise une demande de ressource auprès du Gatekeeper (*Admission et Status*). Il est également chargé de la signalisation et de l'établissement d'un appel (sous-ensemble du protocole Q.931 du RNIS) ;

– H.245, ce protocole permet aux terminaux d'échanger leurs capacités audio/vidéo (codecs supportés, nombre de canaux possibles, modes de conférence acceptés...) et de négocier les canaux logiques de dialogue ;

– T.120, protocole optionnel qui gère l'échange de données entre terminaux H.323.

La passerelle H.323 ou *Gateway* assure l'interface avec une entité H.323 et une entité non H.323 comme les réseaux RNIS (H.320) ou ATM (H.321), la conversion de signalisation H.225/Q.931, l'adaptation des supports et des débits. Chaque passerelle H.323 connaît les numéros E.164 (numéros de téléphone) qui lui sont rattachés, elle dispose en mémoire d'une table de correspondance qui associe à un numéro E.164 une adresse IP, un email ou un alias (figure 16.53). Si le réseau est important, la maintenance des tables peut devenir vite impossible. Ce problème trouve sa solution par l'emploi d'un *Gatekeeper* (garde barrière) qui va centraliser les tables de conversion d'adresses. Chaque *Gateway* vient s'enregistrer sur son *Gatekeeper* et lui déclare toutes ses adresses E.164. Lorsqu'une passerelle doit établir un appel, elle s'adresse au *Gatekeeper* qui lui fournit l'adresse IP de la passerelle destination.

Le garde barrière H.323 ou *Gatekepeer*, système optionnel de gestion des communications établies par les entités H.323 fournit les services :

– translation d'adresses (alias, email, E.164...),

– contrôle des droits des utilisateurs (rejet éventuel d'appel),

– gestion de la bande passante,

– gestion de la passerelle H.323 (management de la zone),

– journalisation des appels.

© Dunod – La photocopie non autorisée est un délit

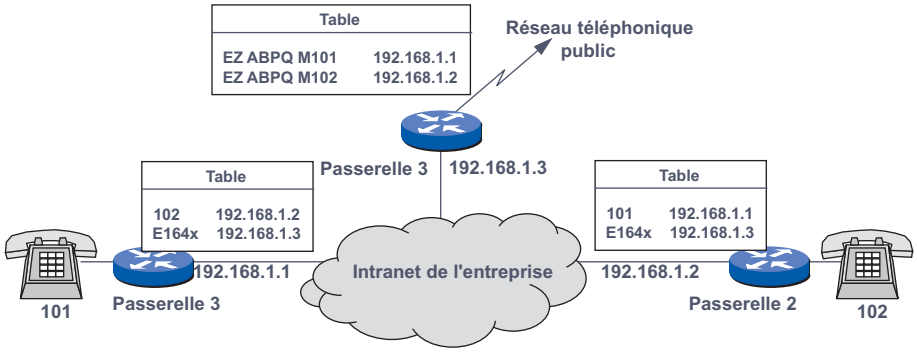


Figure 16.53 Résolution d'adresses par les passerelles.

Enfin, le **MCU** (*Multipoint Control Unit*) aussi optionnel gère l'établissement, le mixage et la diffusion des conférences (contrôle des liaisons multipoints en multicast).

La figure 16.54 décrit la pile protocolaire H.323. la voix est transportée en mode datagramme sur UDP tandis que la signalisation est transportée en mode connecté sur TCP. Les spécifications H.323 correspondent aux niveaux session et supérieurs du modèle de référence, cette approche assure l'interopérabilité des systèmes quel que soit le réseau de transport utilisé.

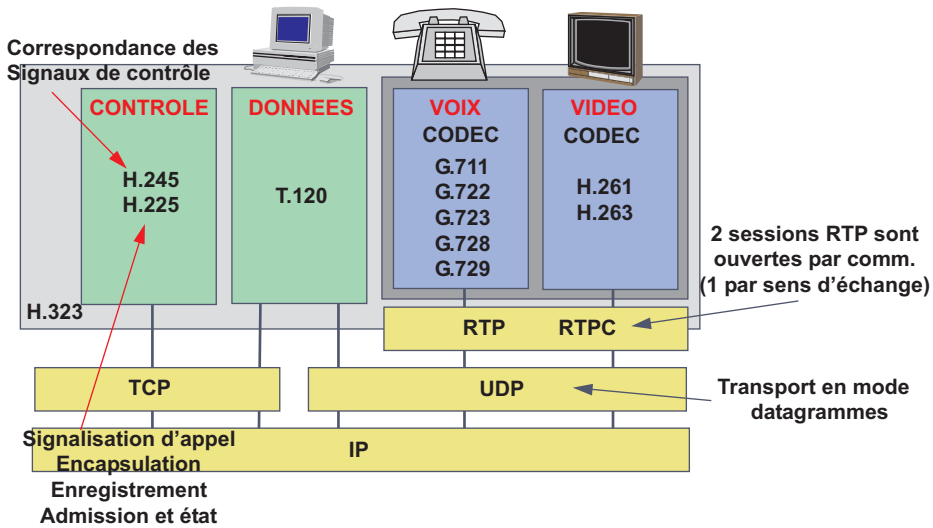


Figure 16.54 La pile protocolaire H323.

La figure 16.55 illustre les relations protocolaires entre un terminal H.323 et un équipement non H.323. Le terminal téléphonique, non H.323, établit un appel en direction du PC multimédia, le routeur (*Gateway* H.323) interprète la numérotation et initialise un appel Q.931 vers l'agent H.323 distant. L'agent H.323 réalise la correspondance entre une adresse E.164 (Q.931) et une adresse IP, il établit un canal de communication entre le demandé et le demandeur.

L'établissement d'une communication H.323 diffère selon que le système utilise ou non un *Gatekeeper*. En mode direct (sans *Gatekeeper*), le terminal qui établit un appel E.164 assure lui-même la traduction d'adresse, la liaison est établie directement par un échange de messages

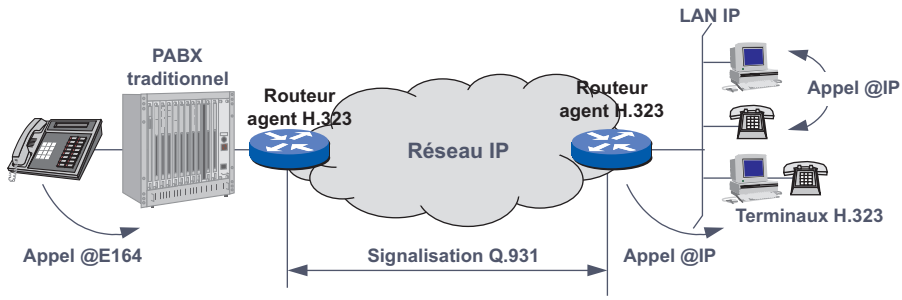


Figure 16.55 Mise en relation selon H.323.

H.225 et H.245. En mode *Gatekeeper*, le terminal appelant interroge, au préalable, le *gatekeeper* pour traduire l'adresse et obtenir l'autorisation d'appeler son correspondant (garantie de bande passante pour accepter un nouveau flux). De même, le correspondant n'accepte l'appel qu'après autorisation de son *Gatekeeper*. La figure 16.56 illustre l'échange de messages H.323.v1.

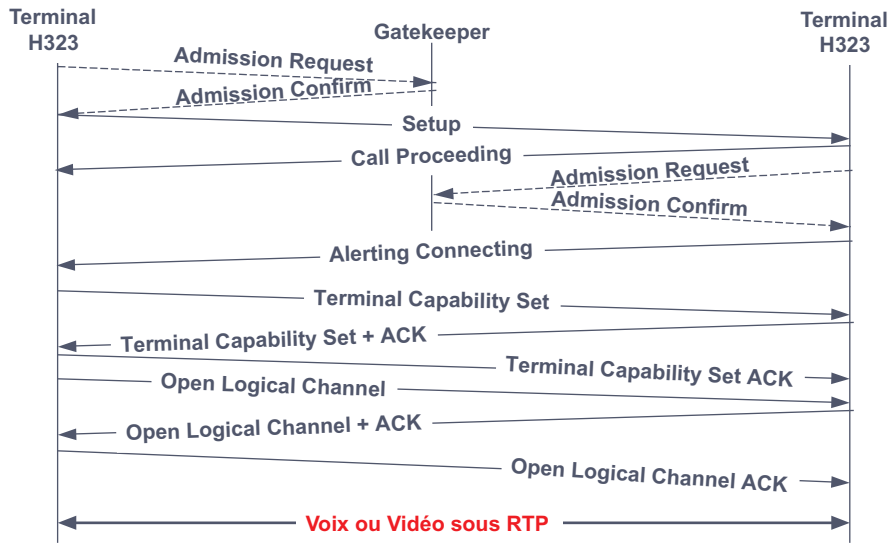


Figure 16.56 Établissement d'appel sous H.323.v1.

Compte tenu de la complexité des échanges, l'établissement d'une communication H.323 peut prendre plusieurs secondes. Aussi, l'UIT a rapidement allégé ce protocole (H.323.v2) en réduisant le nombre de messages échangés. La figure 16.57 illustre l'établissement d'une communication sous H.323.v2.

La principale évolution du protocole H.323 concerne une nouvelle définition des messages dit « *Fast Connect* » qui modifie les messages de connexion (*setup*) en y insérant directement ses différentes capacités, ce message ouvre le canal logique. Le destinataire compare les capacités proposées à ses propres capacités et renvoi un message Q.931 Connect définissant les capacités qui seront utilisées durant la connexion, le canal de retour est alors ouvert.

© Dunod – La photocopie non autorisée est un délit

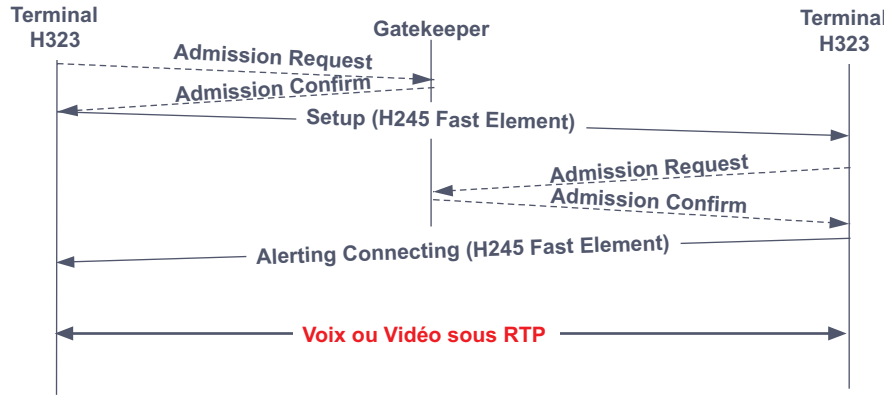


Figure 16.57 Établissement d'un appel sous H.323v2.

16.7.4 Le protocole SIP de l'IETF (RFC 2543)

Actuellement la plupart des solutions développées utilisent la signalisation H.323 (v1, v2 ou v3) d'origine UIT-T. Développé au sein du groupe de travail **MMUSIC** (*Multiparty Multimedia SessIon Control*) de l'IETF, le protocole **SIP** (*Session Initiation Protocol*) beaucoup simple que H.323 pourrait, à terme, remplacer H.323. Les messages SIP sont au format texte, ce qui confère au protocole une grande évolutivité. La figure 16.58 illustre l'architecture SIP.

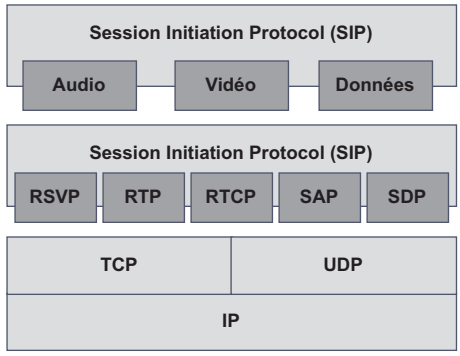


Figure 16.58 Architecture protocolaire SIP.

À l'instar d'H.323, SIP s'appuie sur les protocoles temps réel (RTP et RTCP), il peut éventuellement utiliser RSVP pour obtenir une certaine qualité de service sur le réseau. Le protocole **SAP** *(Session Announcement Protocol*) informe de l'ouverture d'une session multimédia en mode multicast ou non et le protocole **SDP** (*Session Description Protocol*) fournit la description des sessions multimédia.

Basé sur le modèle client serveur, SIP distingue 2 types d'agent : les clients et les serveurs. Les clients ou **UAC** (*User Agent Client*) sont les équipements à l'origine des appels SIP (téléphone IP) ou des passerelles voix. Les passerelles voix SIP ont les mêmes fonctionnalités que les passerelles H323.

Les agents serveurs (**UAS**, *User Agent Server*) sont des équipements classiques (Serveur NT...) qui regroupent les services offerts par SIP. Ce sont :

– les serveurs d'enregistrement utilisés pour la localisation des utilisateurs (*Registar*). Les serveurs d'enregistrement contiennent toutes les caractéristiques des agents SIP autres que les passerelles ;
– les serveurs de délégation (*Proxy Server*) qui gèrent les clients SIP, reçoivent et transmettent les requêtes au serveur suivant (*next-hop server*). Le SIP *Proxy* a un rôle similaire au *Gatekeeper* d'H.323. Un SIP *Proxy* peut interroger un SIP *Registar* ou un DNS pour acquérir les informations d'acheminement de la signalisation et des communications ;
– les serveurs de redirection (*Redirect Server*) qui sur requête transmettent l'adresse du *next-hop server* à l'agent client.

Les messages SIP sont de deux types, les requêtes et les réponses. Les primitives de requêtes sont :

– REGISTER, ce message est émis par un agent pour informer un serveur SIP *Registar* sur sa localisation. Le client fournit une adresse du type Nom@Domaine ;
– INVITE, message d'ouverture de session, émis par un UAC. Ce message peut être transmis directement à l'agent appelé ou à un serveur *Proxy* pour acheminement ;
– BYE, émis par tout agent client pour mettre fin à une session en cours ;
– CANCEL annule une session, ne peut être utilisé que pendant la phase d'ouverture ;
– ACK acquitte un message INVITE et établit la session d'échange ;
– OPTIONS, message d'obtention des capacités (caractéristiques) d'un terminal, similaire à H.245.

Type de messages	Code d'état	Appellation	Commentaires éventuels
INFORMATIONAL	100 180 182	Trying Ringing Queued	Appel pris en compte Retour de sonnerie Mise en attente
SUCCESSFULL	200	OK	Signale que l'appelé a décroché
REDIRECTION	301 305	Moved permanently Use proxy server	Rediriger l'appel vers cette nouvelle position Transiter par ce proxy
CLIENT FAILURE	400 401 420 483 485	Bad request Unauthorised Bad extension Loop Detected Address incomplete	 Emis quand un serveur reçoit une requête pour lui-même
SERVER FAILURE	500 504	Interna Server Error Gateway timeout	
GLOBAL FAILURE	600 603	Busy Decline	 Emis quand l'appelé ne désire pas établir de communication

Figure 16.59 Codes d'état des messages de réponse SIP.

© Dunod – La photocopie non autorisée est un délit

Les messages de réponse sont aussi au nombre de 6, ce sont :

– INFORMATIONAL, simple message de service ;
– SUCCESSFULL, message indiquant que l'action a été menée à bien (succès)...
– REDIRECTION, une autre action doit être conduite pour valider la requête,
– CLIENT FAILURE, message signalant une erreur de syntaxe, la requête ne peut être traitée,
– SERVER FAILURE, message signalant une erreur sur un agent serveur,
– GLOBAL FAILURE, erreur générale, la requête ne peut être traitée par aucun serveur.

Les messages de réponse comportent un code d'état, dont les principaux sont listés dans la figure 16.59.

La figure 16.60 illustre un appel SIP vers un utilisateur qui s'est déplacé. Le client appelant envoie une requête INVITE au serveur proxy auquel il est relié. Ce message contient l'adresse connue du destinataire. Le *Proxy Server* interroge le *Location Server* (DNS, LDAP ou autre) qui lui fournit la nouvelle adresse, le *Proxy* redirige la requête vers la nouvelle adresse de l'appelé (INVITE). Le poste appelé sonne et le poste appelant reçoit un message de retour de sonnerie (SIP 180). L'appelé décroche signifiant ainsi son acceptation de la communication, le système émet alors un message SIP 200 (OK). L'appelant acquitte le message d'acceptation.

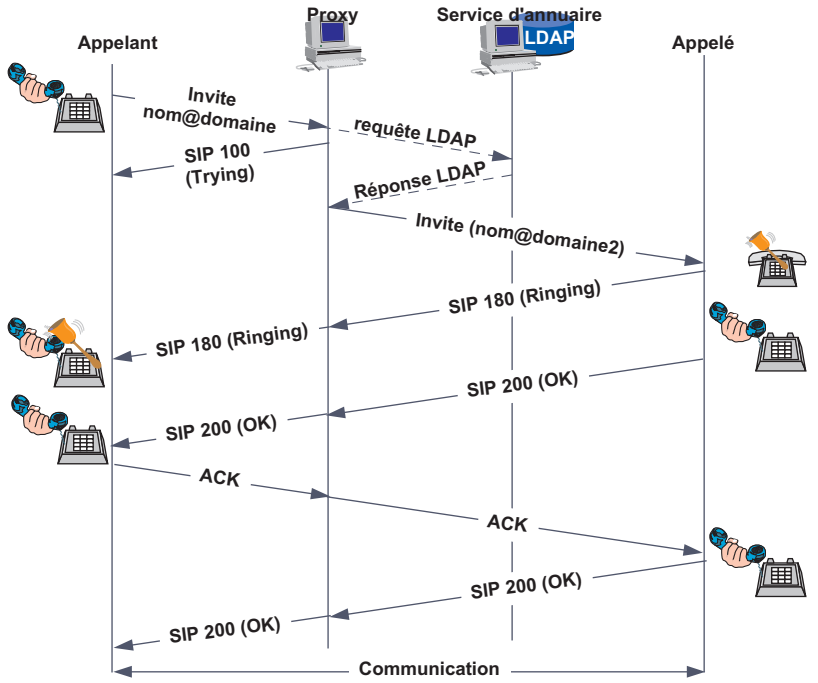


Figure 16.60 Ouverture d'une communication en mode proxy.

Sans *Server Proxy*, l'appelant se serait adressé à un *Redirect Server*, celui-ci consulte le *Location Server* et envoie à l'appelant la nouvelle adresse dans un message **SIP 302** (*moved temporarily*) ou **SIP 301** (*moved permanently*). L'appelant émet alors une requête INVITE directement à l'appelé.

16.7.5 Le protocole MGCP

Un autre protocole entre en compétition **MGCP** (*Media Gateway Control Protocol*) encore plus simple, il centralise « l'intelligence » et peut donc être intégré à des terminaux peu intelligents (clients légers).

MGCP définit plusieurs entités. La passerelle de signalisation (**SG**, *Signalling Gateway*) assure la mise en relation de la signalisation du réseau téléphonique traditionnel, généralement SS7, avec la signalisation utilisée dans le réseau en mode paquets. La passerelle média (**MG**, *Media Gateway*) réalise la paquetisation des signaux voix. Enfin, le contrôleur de passerelle média (**MGC**, *Media Gateway Controller*), cœur du système, pilote les différentes passerelles. D'autres solutions proches ont été proposées. Ces différentes propositions ont conduit à l'élaboration d'un standard commun MEGACO (RFC 3015) pour l'IETF et H.248 pour l'UIT.

16.8 CONCLUSION

La convergence voix/données a donné naissance à une nouvelle génération de réseau dans laquelle la notion de qualité de service devient prépondérante. L'évolution de la téléphonie pour son intégration au réseau donnée est en plein développement. Si la téléphonie sur IP a fait naître l'espoir d'interopérabilité des systèmes, le développement de signalisations propriétaire sur IP, l'opposition H.323 et SIP font reculer cet espoir.

Cependant, le choix se fera autour de H.323 ou de SIP. H.323 bénéficie de son antériorité et d'un fonctionnement assuré, SIP a l'avantage de la simplicité et de l'évolutivité mais il doit encore faire ses preuves.

© Dunod – La photocopie non autorisée est un délit

EXERCICES

Exercice 16.1 Utilisation de l'abaque d'Erlang

Un système à refus dispose de M circuits. Quel est le trafic à soumettre pour un taux de perte 1 %, 10 %, 50 %, lorsque M est respectivement égal à 5, 10 ou 15 ? Déterminer pour chaque valeur, le trafic soumis, écoulé et perdu. (Utiliser l'abaque en annexe.)

Exercice 16.2 Trafic sur un faisceau

Deux systèmes de commutation sont reliés par deux faisceaux de 10 circuits chacun. En supposant un taux de perte de 5 %, on demande :

– le trafic autorisé par chaque faisceau ainsi que le rendement par ligne ;

– le trafic total autorisé par les deux faisceaux ;

– on regroupe les deux faisceaux en un seul de 20 circuits, en supposant le même taux de perte, quels sont le nouveau trafic autorisé et le rendement par ligne ?

Exercice 16.3 Raccordement d'un PABX

Une entreprise a un parc de téléphones en service de 120 postes dont 100 seulement ont accès à l'extérieur. Sachant qu'un utilisateur normal a un trafic téléphonique de 0,12 E se répartissant comme suit :

– 0,04 E en trafic sortant,

– 0,04 E en trafic entrant,

– 0,04 E en trafic interne à l'entreprise.

On vous demande de définir :

1) la capacité de commutation totale, en erlang, du PABX ;

2) le faisceau SPA (appel sortant) sachant que lorsque le faisceau est occupé, les appelants ont la tonalité d'occupation (le taux d'échec ne doit pas dépasser 10 %) ;

3) le faisceau SPB (appel entrant) sachant que lorsque le poste appelé est occupé, l'appelant entend une musique d'attente (le taux d'échec ne doit pas dépasser 2 %) ;

Exercice 16.4 Trafic d'un centre d'appel

Un centre d'appel prévoit que pour une prochaine émission de télévision, il devra accueillir quelques 720 000 appels en 2 heures. Sachant que l'automate de traitement acquiert les données relatives à l'appel en 25 secondes et que le commutateur d'accès met 5 secondes pour prendre en compte une communication, on vous demande de déterminer le nombre de lignes nécessaires et le trafic à écouler en erlang.

Exercice 16.5 Réseau voix/données

Une passerelle voix/données utilise le protocole Frame Relay (FRF11 et FRF12) sur le lien WAN. Sachant que :

– la voix sera compressée selon l'algorithme ADPCM à 16 kbit/s,

– le débit du lien WAN est de 64 kbit/s,

– les paquets de voix seront émis avec une périodicité de 20 ms,

– encapsulation FRF11 et FRF12

Déterminer :

a) le nombre de liens voix utilisables sur cette liaison,

b) le débit maximal restant disponible pour les données,

c) la taille maximale des paquets données en présence de la voix,

d) la gigue maximale introduite par l'insertion d'un paquet données.

Exercice 16.6 Dimensionnement d'un réseau Frame/Relay voix/données

Un réseau Frame Relay utilise des liens loués à 128 kbit/s. Chaque lien supporte 2 canaux voix (ADPCM, 16 kbit/s, fréquence des trames 50 Hz), la signalisation (9,6 kbit/s) et un lien données. Chaque flux utilisera un DLCI différent. On vous demande de définir la valeur du CIR et de l'EIR de chacun des DLCI.

Exercice 16.7 Comparaison H.323 et SIP

Compléter le tableau de la figure 16.51 suivant :

Critères	H.323	SIP
Normalisation		
Transport de la signalisation		
Transport des flux multimédia		
Etablissement de canaux logiques		
Signalisation multicast		
Prioritisation des appels		
Codage des primitives		
Evolutivité		
Détection des boucles		
Gestion des conférences		

Figure 16.61 Comparaison H.323 et SIP.

© Dunod – La photocopie non autorisée est un délit

Chapitre **17**

La sécurité des systèmes d'information

17.1 GÉNÉRALITÉS

La multiplication des moyens d'accès et l'ouverture des réseaux vers l'extérieur de l'entreprise fragilisent le système d'information. Il devient alors la cible d'attaques qui visent non seulement à prendre connaissance ou à modifier l'information mais aussi à paralyser le système. Les moyens mis en œuvre pour le protéger se regroupent sous le vocable de « sécurité des systèmes d'information ». Cependant, il convient de distinguer deux approches de la sécurité :

– la **sûreté de fonctionnement** (*safety*), qui concerne l'ensemble des mesures prises et des moyens utilisés pour se prémunir contre les dysfonctionnements du système ;
– la **sécurité** (*security*), proprement dite, qui regroupe tous les moyens et les mesures prises pour mettre le système d'information à l'abri de toute agression.

17.2 LA SÛRETÉ DE FONCTIONNEMENT

17.2.1 Principes généraux de la sûreté

L'indisponibilité d'un système peut résulter de la défaillance des équipements de traitement (panne), de la perte d'information par dysfonctionnement des mémoires de masse, d'un défaut des équipements réseau, d'une défaillance involontaire (panne) ou volontaire (grève) de la fourniture d'énergie mais aussi d'agressions physiques comme l'incendie et les inondations.

17.2.2 Les systèmes à tolérance de panne

La fiabilité matérielle est obtenue par sélection des composants mais surtout par le doublement des éléments principaux, ces derniers systèmes sont dits à tolérance de panne (*fault tolerant*).

La redondance peut être interne à l'équipement (alimentation...) ou externe. Les systèmes à redondance utilisent les techniques de **mirroring** et/ou de **duplexing**.

Le *mirroring* est une technique dans laquelle le système de secours est maintenu en permanence dans le même état que le système actif (miroir). La *duplexing* consiste à avoir un équipement disponible qui prend automatiquement le relais du système défaillant.

Le *mirroring* disques consiste à écrire simultanément les données sur deux disques distincts. En cas de défaillance de l'un, l'autre continue d'assurer les services disques. La panne est transparente pour l'utilisateur. Après remplacement du disque défectueux, le système reconstruit automatiquement le disque miroir (figure 17.1). Évolution du mirroring, le duplexing consiste à relier chaque disque miroir à un contrôleur disque différent. Le duplexing répartit le trafic sur les canaux disques et, par conséquent, améliore les performances. Le duplexing protège à la fois contre les défaillances du disque et contre celles du contrôleur.

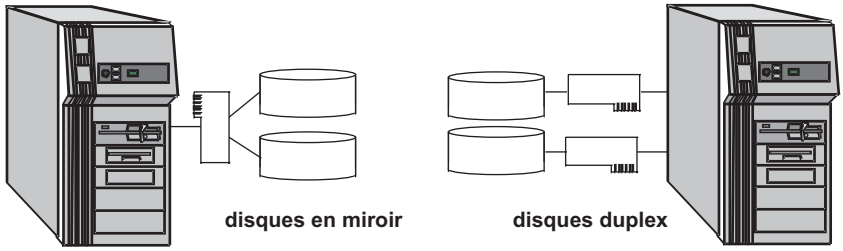


Figure 17.1 Le mirroring et de duplexing de disques.

Pour les mémoires de masse, les stratégies de tolérance de panne (**RAID**, *Redundant Array of Independant Disk*) sont classées en six niveaux. En pratique, seuls deux niveaux sont utilisés (niveau 1 et 5). Le tableau de la figure 17.2 présente une synthèse des systèmes RAID.

Niveau	Description
RAID 0	Le RAID 0 est un système d'agrégats de bandes (*stripping*). Les données sont séparées en blocs répartis selon un ordre prédéterminé entre tous les disques de la grappe. En écrivant les différents blocs simultanément, RAID 0 améliore les performances, mais ce n'est pas un système à tolérance de panne (pas de redondance).
RAID 1	Système de disques miroirs, RAID 1 améliore les performances en lecture (lectures simultanées). Il n'a pas d'incidence sur les performances en écriture (écriture en parallèle).
RAID 2	Correspond à l'exploitation des disques par bandes (RAID 0), avec un code de correction d'erreur (ECC). Un ou plusieurs disques sont dédiés à la sauvegarde des ECC.
RAID 3	Reprend les principes du RAID 2 et ajoute un contrôle de parité.
RAID 4	Similaire au RAID 3 mais les codes de contrôle de parité sont stockés sur un disque particulier.
RAID 5	Semblable au RAID 4 mais les codes de contrôle de parités sont répartis sur tous les disques de la grappe. En cas de défaillance d'un disque, les données de celui-ci sont reconstituées. Il n'y a pas d'interruption de service. Lors du remplacement du disque défaillant, celui-ci est reconstruit automatiquement par le système.

Figure 17.2 Synthèse des systèmes RAID.

L'utilisation des systèmes de sécurité du type RAID ne dispense pas de réaliser des sau-

vegardes régulières, seule solution capable de protéger les données d'un effacement accidentel (erreur d'un utilisateur). Les sauvegardes peuvent être réalisées sur une autre machine du réseau dédiée à cet usage, sur des mémoires de masses distantes ou sur des bandes de sauvegardes conservées dans un autre local.

La mise en duplex d'équipement comme les serveurs représentent le niveau le plus élevé. Chaque serveur (figure 17.3) constitue un sous-système géré par le système d'exploitation. L'utilisateur est connecté à l'un des serveurs. Toutes les opérations effectuées sur l'un sont recopiées, via un canal à haut débit, sur l'autre. En cas de défaillance d'un serveur, la connexion de l'utilisateur est basculée sur l'autre. La panne est totalement transparente.

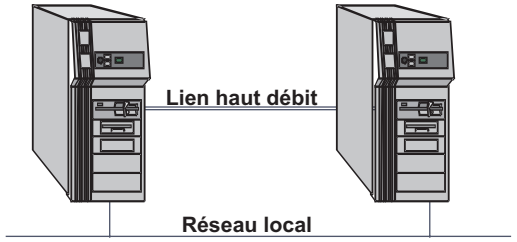


Figure 17.3 Duplexing de serveurs.

La sécurité des moyens de transport est généralement réalisée par la redondance des liens obtenue par le maillage du réseau ou par le doublement des raccordements au réseau de l'opérateur. Dans ce dernier cas, il faut veiller à ce que le cheminement des liens, leur point de raccordement au réseau de l'opérateur et les pénétrations dans les locaux informatiques soient distincts. En fonctionnement normal le réseau peut utiliser les deux liens (équilibrage de charge), en cas de rupture d'un lien, le trafic sera intégralement écoulé sur le lien restant (fonctionnement dégradé). Compte tenu des coûts, de nombreuses entreprises préfèrent utiliser une connexion de secours établie à la demande. Dans ce cas, c'est le réseau téléphonique qui est utilisé comme lien de secours. Une communication est établie en agrégeant, selon le besoin, plusieurs canaux B (figure 17.4).

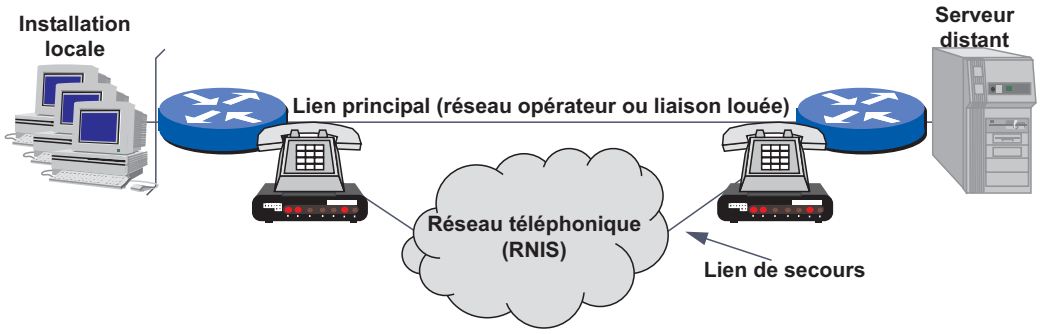


Figure 17.4 Duplication de la ligne de transmission.

17.2.3 La sûreté environnementale

L'indisponibilité des équipements peut résulter de leur défaillance interne mais aussi d'événements d'origine externe. Le réseau électrique est la principale source de perturbation (coupures, microcoupures, parasites, foudre...). Des équipements spécifiques peuvent prendre le

© Dunod – La photocopie non autorisée est un délit

relais en cas de défaillance du réseau (onduleur *off-line*) ou constituer la source d'alimentation électrique permanente du système (onduleur *on-line*). Ces équipements fournissent, à partir de batteries, le courant électrique d'alimentation du système.

Les onduleurs de type *off-line* (figure 17.5) sont surtout destinés à alimenter des systèmes autonomes (protection d'un poste de travail...). En présence du courant secteur, le convertisseur chargeur de batteries maintient la charge de celles-ci. L'équipement est alimenté directement par le réseau électrique. En cas de coupure, le commutateur bascule en quelques millisecondes, et le système est alors alimenté par le convertisseur courant continu/courant alternatif.

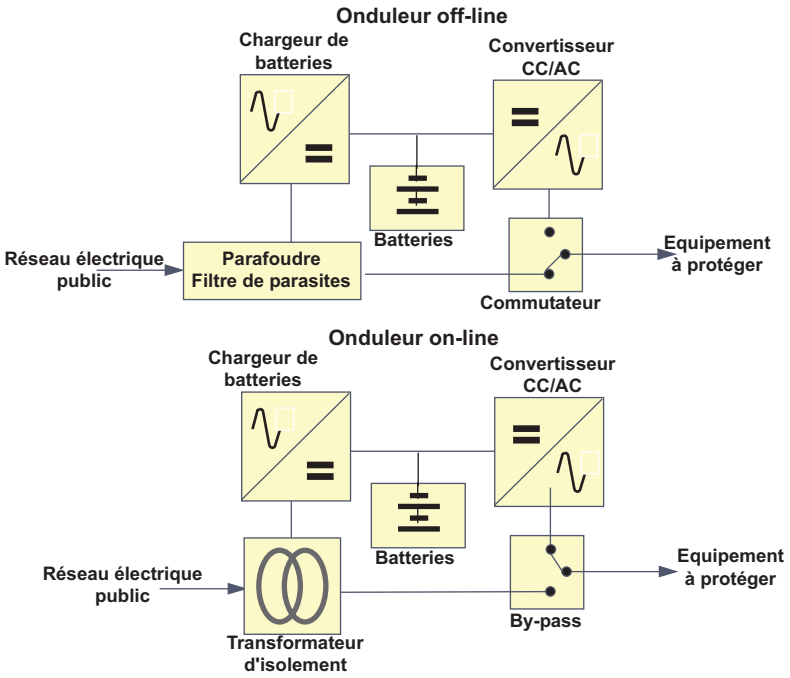


Figure 17.5 Principes des onduleurs.

Les onduleurs *on-line* alimentent en permanence le système externe. Le courant alternatif fourni est parfaitement stabilisé en amplitude et fréquence. Le système est protégé des micro-coupures. En cas de panne de l'onduleur ou d'une surcharge, un commutateur automatique (*by-pass*) bascule le système sur le réseau électrique.

L'autonomie de tels systèmes est généralement fixée à 20 minutes Pour les systèmes devant assurer un fonctionnement permanent, un groupe électrogène se substitue au réseau d'énergie public en cas de défaillance.

La durée de fonctionnement d'un équipement est aussi en relation directe avec les contraintes thermiques qu'il subit, aussi, les locaux informatiques doivent-ils être climatisés (20 à 23 °C). La climatisation doit assurer une ventilation forcée des équipements avec un taux de poussière maximal (200 $\mu g/m^3$/24 heures), maintenir un degré hygrométrique (H) correct (40 % < H < 85 %). La salle doit être protégée contre les agressions extérieures comme les intrusions, mais aussi contre les éléments (inondation et incendie).

En fonction des moyens mis en œuvre et de la fiabilité de chacun des éléments, on peut

déterminer la probabilité pour que le système fonctionne correctement pendant un laps de temps donné (disponibilité).

17.2.4 Quantification

Définitions

La **fiabilité** d'un système est la probabilité pour que le système fonctionne correctement pendant une durée donnée dans des conditions définies. La **maintenabilité** d'un système est la probabilité de retour à un bon fonctionnement dans un temps donné. Les différentes pannes pouvant être catalectiques (l'élément fonctionne ou ne fonctionne pas), ou aléatoires (défaillance statistiquement indépendante d'une précédente, la panne d'un élément n'affecte pas les autres). Le comportement d'un système peut être décrit dans le temps comme une suite d'états de bon et de mauvais fonctionnement.

On appelle **MTTR**, (*Mean Time To Repair*, temps moyen de toute réparation), le temps nécessaire à la remise en état du système et **MTBF** (*Mean Time Between Failure***,** temps moyen de bon fonctionnement) le temps moyen entre deux pannes successives.

Relation entre disponibilité et MTTR/MTBF

La disponibilité (*Avaibility*) est définie comme étant le rapport :

$$A = \frac{MTBF}{MTBF + MTTR}$$

et l'indisponibilité comme en étant le complément (le matériel est indisponible lorsqu'il n'est plus disponible) :

$$I = 1 - A = \frac{MTTR}{MTBF + MTTR} \quad \text{avec} \quad \frac{I}{A} = \frac{MTTR}{MTBF}$$

Pour rendre un système plus efficace, on peut jouer sur 2 valeurs : augmenter la MTBF, les composants réseaux seront alors plus onéreux ou diminuer les temps d'indisponibilité et c'est la maintenance qui devient plus coûteuse.

Les structures de fiabilité

Selon les relations existantes entre les différents composants du système (figure 17.6), la résistance à la défaillance sera plus ou moins grande. Généralement, on distingue quatre structures de base :

- la structure série sans redondance : dans un tel système lorsque l'un des composants tombe en panne, l'ensemble du système est indisponible ;
- la structure avec duplication de systèmes : dans une telle organisation, la panne d'un seul composant n'affecte pas le fonctionnement global du système ;
- la structure avec duplication de toutes les unités : ici la panne de plusieurs composants ne rend pas le système indisponible ;
- enfin, la structure avec duplication partielle : compte tenu des coûts engendrés par la duplication totale, seuls sont dupliqués, ici, les systèmes les plus sensibles.

© Dunod – La photocopie non autorisée est un délit

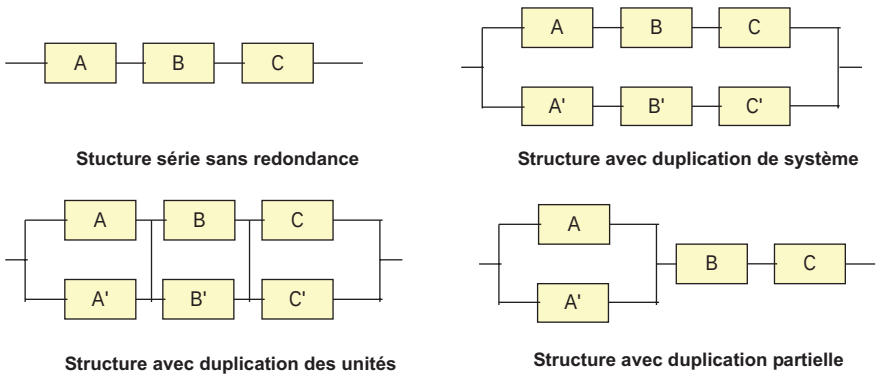


Figure 17.6 Les structures de fiabilité.

La mesure de la disponibilité globale d'un système dépend de sa structure. Deux structures élémentaires sont à la base de tout système : la structure série et la structure parallèle (figure 17.7).

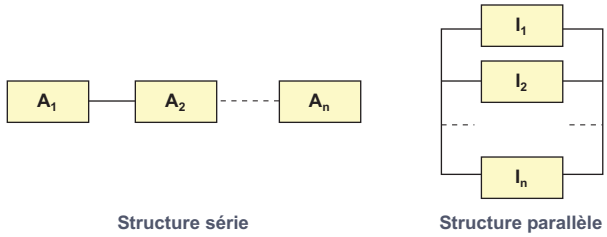


Figure 17.7 Les structures élémentaires.

➤ La structure série :

La disponibilité résultante est plus petite que celle du composant le plus faible :

$$A_t = A_1 \cdot A_2 \cdot \ldots \cdot A_n$$

L'indisponibilité est alors :

$$I_t = 1 - A_t = 1 - [(1 - I_1) \times (1 - I_2) \ldots \times (1 - I_n)]$$

Si A $\approx$ 1, c'est-à-dire que I est très petit on peut écrire :

$$I_t = \sum_{1}^{n} I_n$$

On montrerait aussi que :

$$MTBF_s = \frac{1}{\sum_{i=1}^{i=n} (1/MTBF_i)}$$

➤ La structure parallèle

L'indisponibilité du système est plus petite que celle du composant qui a la plus faible indisponibilité :

$$I_t = I_1 \cdot I_2 \cdot ... \cdot I_n$$

La disponibilité est alors :

$$A_t = 1 - I_t = 1 - [(1 - A_1) \times (1 - A_2)... \times (1 - A_n)]$$

De même, on montre que :

$$MTTR_p = \frac{1}{\sum_{i=1}^{i=n} (1/MTTR_i)}$$

17.3 LA SÉCURITÉ

17.3.1 Généralités

L'ouverture des réseaux de l'entreprise au monde extérieur, la décentralisation des traitements et des données ainsi que la multiplication des postes de travail accroissent les risques de dénaturation des systèmes et d'altérations des données. Les menaces peuvent se regrouper en cinq catégories, celles qui visent à :

- prendre connaissance des données sans y être habilité (**confidentialité**),
- altérer les données (**intégrité**),
- mystifier les correspondants par usurpation d'identité (**authentification**),
- nier l'existence d'une transaction (**non-désaveu** ou non-répudiation),
- paralyser les systèmes (**déni de service**).

Les mécanismes mis en œuvre peuvent se répartir en deux techniques : celles qui tendent à protéger les données et celles qui tendent à protéger les systèmes.

17.3.2 La protection des données

D'une manière générale, la confidentialité est assurée par le chiffrement des messages, l'authentification des correspondants par un échange de mots de passe plus ou moins simple, enfin le non-désaveu est garanti par un système d'accusé de réception ou par l'intervention d'un tiers (le notaire) qui mémorise et authentifie les transactions (notarisation).

Notions de cryptographie

➤ Généralités

Le chiffrement est une technique destinée à rendre les données inintelligibles pour les tiers non autorisés. L'opération de brouillage du texte s'effectue à partir d'une clé (clé de chiffrement).

© Dunod – La photocopie non autorisée est un délit

La figure 17.8 illustre une chaîne de cryptage. Le message en clair est codé (chiffré) à l'aide d'une clé de chiffrement ; seul, le cryptogramme (message chiffré) est transmis sur le réseau. Le destinataire du message effectue le décryptage à l'aide d'une clé de déchiffrement.

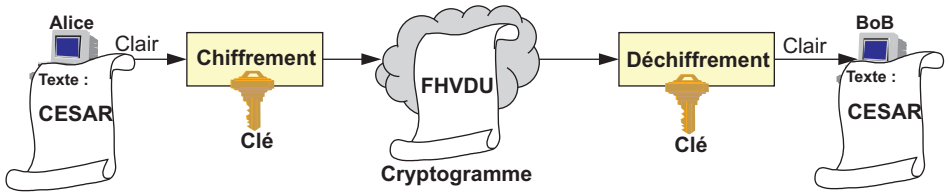


Figure 17.8 Principe de la cryptographie.

Les techniques de cryptographie sont utilisées pour :

– assurer la confidentialité des données (algorithme de chiffrement),
– garantir l'intégrité des données (algorithme de hachage),
– authentifier l'émetteur des données (algorithme de signature numérique).

➤ Les méthodes de chiffrement symétrique

Les systèmes à **clés symétriques** ou secrètes utilisent une clé de chiffrement et une clé de déchiffrement identiques, convenues par avance et conservées secrètes. Ce système ne permet pas d'identifier l'interlocuteur distant. Ces algorithmes utilisent deux techniques : la substitution et la transposition indépendamment ou successivement.

Le code de César est le plus vieil algorithme de chiffrement symétrique à substitution connu. Son principe est extrêmement simple, il suffit de substituer à chaque lettre du clair, une lettre de l'alphabet obtenue par simple translation (clé secrète) dans l'alphabet. Par exemple, si la translation est de 3, la lettre A est remplacée par la lettre D, la lettre B par E... La figure 17.9 illustre l'application de ce codage au mot « CESAR », la clé étant fixée à 3. Le clair « CESAR » donne alors pour chiffre le message « FHVDU ».

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C			•	•	•	F																				
E					•	•	•	H																		
S																			•	•	•	•	V			
A	•	•	•	D																						
R																		•	•	•	U					

Figure 17.9 Décalage de César.

Le principe des codes à permutation ou transposition consiste à modifier, selon une loi prédéfinie, l'ordre des caractères. Les méthodes de pliage constituent un exemple simple des codes à transposition. Ils consistent à écrire le message d'origine (clair) dans une matrice comportant autant de colonnes que la clé de caractères. Le cryptogramme est obtenu en écrivant, en ligne, le clair dans la matrice puis en lisant cette matrice en colonnes dans l'ordre défini par la clé. Soit, par exemple, le message « UNE PLANCHE A VOILE » et la clé de codage 4312 :

La clé a une longueur de 4, on crée une matrice de 4 colonnes puis on inscrit le message horizontalement (sans les blancs). Enfin, on lit la matrice verticalement dans l'ordre de la clé (figure 17.10). On obtient le message : PCVE ENAL ULHO NAEI.

À l'inverse, pour déchiffrer un message, il suffit de l'écrire verticalement dans l'ordre de la clé et de lire horizontalement.

↓ Lecture

Ecriture →	1	2	3	4
	U	N	E	P
	L	A	N	C
	H	E	A	V
	O	I	L	E

Figure 17.10 Matrice de chiffrement et de décryptage.

Le **DES** (*Data Encryption Standard*) d'origine IBM (Karl Meyer 1977) est l'algorithme à clé symétrique le plus connu. Il consiste en une suite de substitutions (DES-S) et de transpositions, ou permutations (DES-P), par bloc de 64 bits. La figure 17.11 illustre de manière simple le principe d'un tel code. Utilisant une clé de 56 bits (64 bits dont 8 de parité), le DES est aujourd'hui facilement « cassable », il est remplacé par le triple DES (3DES, application de 3 DES successivement avec 3 clés indépendantes).

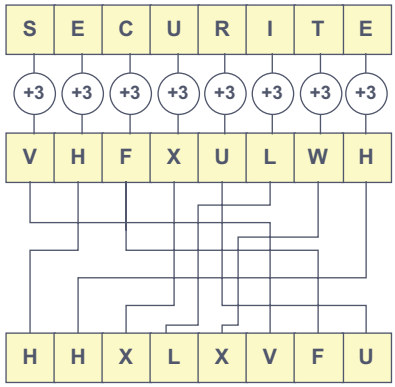


Figure 17.11 Principe du DES.

Les algorithmes de cryptographie à clé secrète demandent relativement peu de puissance, le temps de calcul est compatible avec un échange interactif de messages. Cependant, la découverte de la clé secrète donne accès à l'information. Dans de tels algorithmes, le secret (la clé) doit être transmis d'où les risques d'interception ou alors préalablement connu des deux correspondants et dans ce cas c'est un de trop !

➤ Les méthodes de chiffrement asymétrique

Evitant la diffusion de clés, les systèmes à **clés asymétriques** utilisent deux clés, l'une est connue de tous (**clé publique**), l'autre n'est connue que de l'un des correspondants (**clé secrète**). Le message chiffré avec l'une ne peut être déchiffré qu'avec l'autre. Les deux clés sont reliées mathématiquement entre elles, mais l'utilisation de grands nombres rend ce lien pratiquement impossible à retrouver. La figure 17.12 illustre ce mécanisme.

© Dunod – La photocopie non autorisée est un délit

Figure 17.12 Principe de la cryptographie à clé publique.

Le système de cryptographie à clé asymétrique le plus répandu, le **RSA** du nom de ses inventeurs (*Rivest, Shamir et Adleman*) repose sur l'arithmétique des grands nombres. La fonction de chiffrement est de la forme :

$$\text{Crypte} = [\text{Clair}^{\text{clé C}} \text{ modulo } n]$$

Crypte : message codé — Clair : message à coder

clé C : clé de chiffrement — n : produit de nombres premiers.

La fonction de déchiffrement est identique :

$$\text{Clair} = [\text{Crypte}^{\text{clé D}} \text{ modulo } n]$$

La figure 17.13 illustre le chiffrement et déchiffrement pour un système dont les paramètres seraient C = 3, D = 7 et n = 33.

Clair	N = Clair ^{C}	Crypte = N mod n	N = Crypte ^{D}	Clair = N mod n
0	0	0	0	0
1	1	1	1	1
2	8	8	2 097 152	2
3	27	27	10 460 353 203	3
4	64	31	27 512 614 111	4
5	125	26	8 031 810 176	5

Figure 17.13 Exemple de chiffrement et de déchiffrement à clé asymétrique.

Fondés sur la difficulté de factoriser des nombres premiers, les systèmes à clé publique permettent d'assurer la confidentialité des données mais aussi d'authentifier l'émetteur d'un message.

➤ L'authentification de l'émetteur

Un message chiffré avec la clé publique n'est déchiffrable qu'à l'aide de la clé privée, cela assure la confidentialité mais ne permet pas d'authentifier l'auteur du message. L'authentification de l'émetteur peut être obtenue en chiffrant le message avec la clé secrète et en le déchiffrant avec la clé publique (figure 17.14).

Si Alice, à l'aide de la clé publique de Bob, déchiffre le message c'est que celui-ci a bien été codé à l'aide de la clé privée de Bob, donc Bob est bien l'émetteur du message. Ce procédé ne garantit pas la confidentialité des messages, tout possesseur de la clé publique peut déchiffrer le message, il ne garantit que l'origine (le détenteur de la clé privée), c'est un système de signature de messages.

Figure 17.14 Principe du PgP.

➤ Protocole d'échange de clés Diffie-Hellman

La cryptographie à clé publique nécessite une puissance de calcul importante. Le DES est entre 100 fois (implémentation logicielle) et 1 000 fois (implémentation *hardware*) plus rapide que le RSA. Le protocole d'échange de clés de Diffie-Hellman permet de construire une clé secrète (clef de session) sans que celle-ci circule sur le réseau. L'initiateur de l'échange transmet à son correspondant deux nombres grands et premiers (g, n). Les correspondants déterminent une clé privée, tenue secrète. Chacun, à partir de g, n et de sa clé secrète (nombres aléatoires A et B) génère une clé publique et la communique à l'autre. Puis, à partir de sa clé privée, de sa clé publique et de la clé publique de son correspondant, calcule la clé de session (figure 17.15).

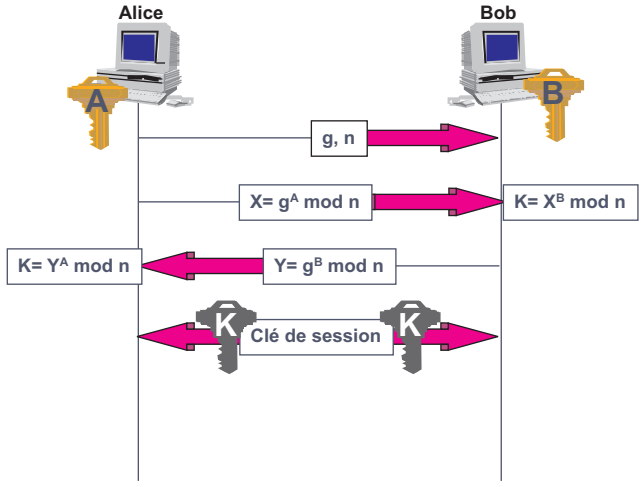


Figure 17.15 Principe de l'échange de Diffie-Hellman.

Le protocole de Diffie-Hellman permet de sécuriser l'échange de clé, cette technique est utilisée dans IPSec (*IP Secure*)

➤ Contrôle d'intégrité du message

Pour vérifier l'intégrité d'un message, on utilise une technique similaire à celle du CRC (*Cyclic Redundancy Check*). Une fonction dite de hachage (**hash**) est appliquée au contenu du message. Le résultat obtenu ou **digest** (résumé, sceau...) est joint au message à transmettre, il est recalculé par le destinataire. Si le résultat du calcul local est identique au digest reçu, le message n'a pas été altéré (figure 17.16).

La fonction de hachage doit garantir qu'il est impossible à partir du digest de retrouver le message initial (non retour arrière ou *one-way hash*) et qu'il doit être quasi impossible que

© Dunod – La photocopie non autorisée est un délit

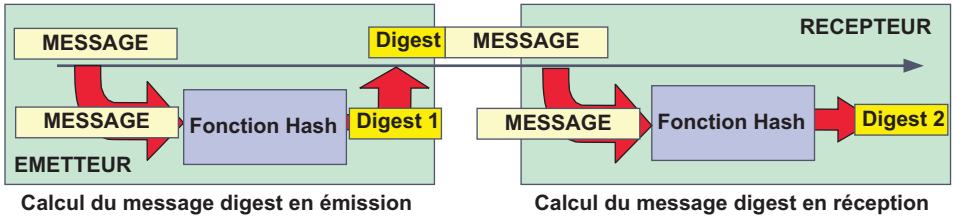


Figure 17.16 Principe de détermination du « digest ».

deux messages différents ne donnent le même digest (résistance à la collision). Le digest a une longueur de 128 bits (MD2 à MD5, *Message Digest X*, défini par Ron Rivest et normalisé par la RFC 1321) ou de 160 bits (SHA-1, *Secure Hash Algorithm*).

➤ Signature numérique d'un message

En combinant un système de cryptographie et une fonction de hachage, on peut à la fois garantir l'intégrité du message et son authentification (**MAC**, *Message Authentification Code*). Selon que l'on utilise un système de cryptographie à clé sécrète ou publique on obtient une signature numérique dite symétrique ou asymétrique.

Dans le système à signature symétrique, l'émetteur calcule le digest sur la concaténation de la clé secrète et du message (figure 17.17). Le destinataire procède de même, si le digest trouvé est identique à celui qui a été reçu, c'est d'une part que le message n'a pas été altéré et d'autre part qu'il a bien été émis par l'autre possesseur de la clé partagée.

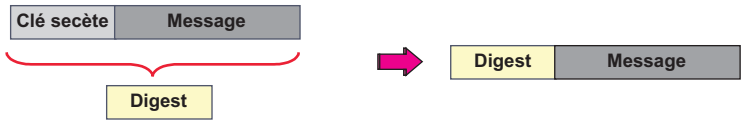


Figure 17.17 Calcul d'une signature numérique symétrique.

Dans le système à signature asymétrique, le digest est calculé sur le message puis chiffré à l'aide de la clé privée de l'émetteur, le résultat est joint au message envoyé (figure 17.18). Le destinataire calcule le digest sur le message, déchiffre le digest reçu à l'aide de la clé publique de l'émetteur. Si les résultats sont identiques, le message n'a pas été altéré et l'émetteur est identifié, c'est le possesseur de la clé publique.

Figure 17.18 Calcul d'une signature numérique asymétrique.

Les systèmes à signature numérique permettent d'assurer l'authentification (qui est l'émetteur du message) et l'intégrité de celui-ci (le message n'a pas été modifié par un tiers). N'ayant besoin d'aucun secret partagé l'authentification par signature numérique asymétrique est plus efficace. Cependant, elle nécessite une puissance de calcul supérieure et ralentit les échanges de messages. Le protocole IPSec utilise les deux systèmes, les correspondants s'authentifient d'abord par signature numérique asymétrique, puis les échanges suivants sont authentifiés par signature symétrique.

Sécurisation des échanges

➤ Usurpation d'identité

L'un des problèmes de la cryptographie à clef publique est la possible intervention d'une tierce personne (figure 17.19). Lorsqu'Alice veut entrer en relation avec Bob en utilisant un système de cryptographie à clé publique, elle doit demander à Bob sa clé publique. Cet échange peut être intercepté par Charlie, un intrus malveillant, qui peut répondre en lieu et place de Bob avec sa propre clé publique. De cette manière, il pourra se substituer à Bob lors des prochains échanges, Alice étant persuadée que les messages proviennent bien de Bob. La même opération est réalisée lorsqu'Alice envoie sa clé publique à Bob. Cette attaque est connue sous le nom de « *Man in the milde* ».

Figure 17.19 Substitution d'identité.

Afin d'éliminer la substitution d'identité, les clés publiques sont disponibles sur un serveur de clés publiques (annuaire) et donc accessibles à tous les utilisateurs, encore faut-il que soit confirmée la relation clé publique/possesseur. C'est l'intervention d'un tiers de confiance (**CA**, *Certificate Authority*) qui garantit la correspondance entre une clé publique et son propriétaire par la délivrance d'un certificat. Le certificat contient l'identifiant d'un utilisateur et sa clé publique, le certificat est signé avec la clé privée de l'autorité d'authentification. L'autorité de certification peut être interne à l'entreprise (disponible sur l'intranet) ou être un prestataire de service de certification.

➤ Exemple d'infrastructure de sécurité, la PKI

La **PKI** (*Public-Key Infrastructure*) est un ensemble de protocoles et de services associés qui assurent la gestion des clés publiques. Les différentes fonctions à assurer sont :

– La génération des clés : le système génère et gère deux types de clés, les clés de chiffrement et les clés de signature numérique des messages. La paire de clés publique/privée peut être

© Dunod – La photocopie non autorisée est un délit

générée par le CA ou le client. Lorsqu'un client génère lui-même ses clés, il séquestre celle-ci chez le CA en vue d'obtenir la délivrance d'un certificat.

– L'archivage des clés et des certificats (séquestre) : l'agent de séquestre doit assurer le contrôle des accès aux clés privées.
– La délivrance des certificats et clés : celle-ci s'accompagne de la vérification de l'identité du demandeur.
– La gestion des listes de révocation (**CRL**, *Certificate Revocation List*), c'est-à-dire la liste des clés déclarées invalides avant leur date d'expiration.

La figure 17.20 illustre le fonctionnement d'une infrastructure PKI, dans le cas simple où le client génère lui-même son couple de clés. Bob formule une demande de certificat auprès d'une autorité de certification (CA). Celui-ci, après vérification de l'identité de Bob, lui délivre un certificat et le signe avec sa clé privée. Bob envoie son certificat à Alice et le signe avec sa clé privée. Alice apprend ainsi la clé publique de Bob (validée par la signature numérique du CA) et vérifie auprès du CA la validité du certificat (consultation de la liste des révocations, CRL). Elle vérifie ensuite que Bob est bien l'émetteur du message par lecture de la signature de Bob (utilisation de la clé publique de Bob).

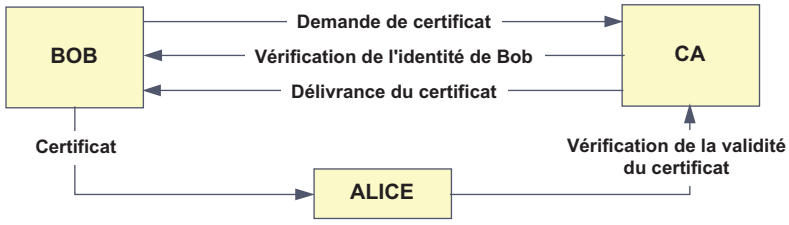


Figure 17.20 Principe des échanges sous PKI.

La délivrance de certificats numériques est normalisée par l'UIT (X.509, actuellement version 3). Un certificat **X.509** identifie la norme (V3 actuellement) et comporte entre autres les informations suivantes :

– un numéro de série unique,
– un identifiant de l'algorithme de signature utilisé,
– le nom de l'émetteur,
– la période de validité,
– la clé publique du sujet,
– l'identifiant de l'émetteur (CA),
– l'identifiant unique du sujet,
– un champ d'extension pouvant comporter du texte, une image...
– la signature de l'émetteur (CA),
– un second champ d'extension a été ajouté par la version 3, il permet notamment d'indiquer le nom et le prénom du titulaire, ses coordonnées...

Le protocole de sécurité de l'environnement IP (IPSec) utilise des certificats X.509 pour l'authentification et le chiffrement.

Sécurité et protocole de transmission

➤ La sécurité et le protocole PPP (RFC 1334)

Rappelons que le protocole PPP (*Point to Point Protocol*) assure quatre fonctionnalités (figure 17.21), la négociation des paramètres de connexion, l'affectation d'adresse IP, la sécurisation des échanges par authentification des communicants et enfin le transfert de données.

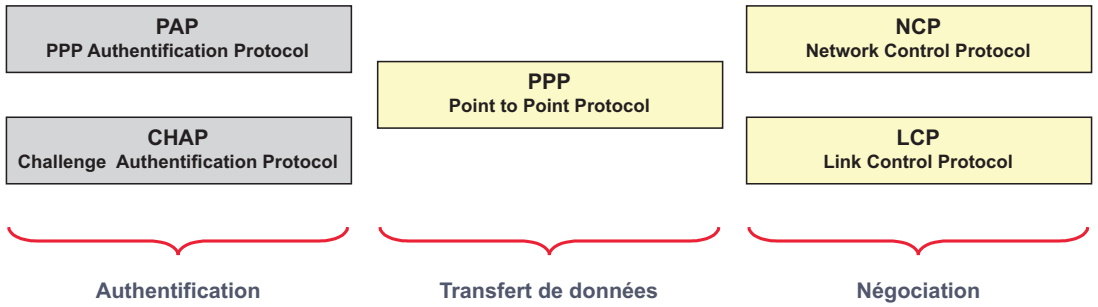


Figure 17.21 PPP et ses sous-protocoles.

Lorsque les paramètres liaison et réseau sont définis, si l'entité LCP a négocié une phase d'authentification, PPP procède à l'identification des entités communicantes.

PAP (*Password Authentification Protocol*) consiste en un simple échange de mots de passe en clair sur le réseau. Cette méthode est très vulnérable, les mots de passe peuvent être écoutés sur la liaison. Un intrus pourra usurper l'identité d'un des interlocuteurs.

CHAP (*Challenge Handshake Authentification Protocol*), ce protocole repose sur l'échange de messages cryptés selon une clé secrète (algorithme à clés symétriques) qui ne circule pas sur le réseau. L'identificateur envoie un message en clair à l'interlocuteur distant (Challenge). Celui-ci crypte le message avec la clé secrète et le renvoie à l'identificateur (sceau). Si le message reçu est correctement crypté, l'identificateur en conclut que son interlocuteur est bien celui qu'il prétend être. La séquence exécutée dans les deux sens peut être répétée plusieurs fois au cours de la session (échange de sceaux).

➤ Sécurisation des échanges sur le web

S-HTTP (Secure HTTP)

S-HTTP introduit la cryptographie au niveau HTTP dont elle constitue une extension. S-HTTP organise la session en trois étapes :

– l'authentification, par échange de mots de passe ;
– la négociation, phase où les interlocuteurs négocient le mode de cryptage à utiliser (DES, RSA...) ;
– la transaction, échange de messages cryptés selon le mode prédéfini.

La cryptographie est mise en œuvre par des scripts CGI ou par des « *daemon* » HTTP (*plug in*).

© Dunod – La photocopie non autorisée est un délit

SSL (Secure Sockets Layer)

Développé par Netscape Communication et intégré aux principaux navigateurs, **SSL** constitue une couche insérée entre la couche application et la couche TCP (figure 17.22). *Secure Sockets Layer* procède en quatre étapes :

– le client s'identifie auprès du serveur Web ;
– le serveur Web répond en communiquant sa clé publique ;
– le client génère alors une clé secrète, la chiffre à l'aide de la clé publique du serveur et la communique à ce dernier ;
– la clé ainsi attribuée est utilisée durant toute la session.

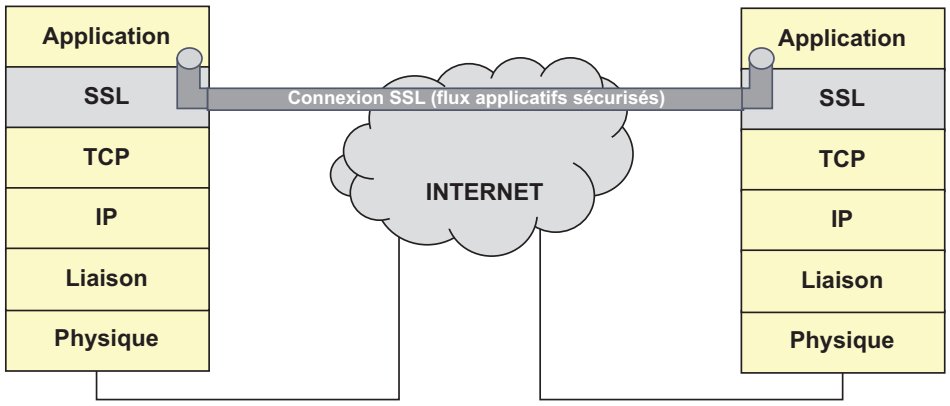


Figure 17.22 Principe de l'architecture de SSL.

SSL crée une connexion qui permet un échange sécurisé dans le réseau. Cependant, le système n'est pas infaillible. En effet, la clé secrète est générée à partir de l'horloge de la machine, ce qui permet de la trouver en quelques minutes.

➤ IP Security

Non limité aux échanges via un navigateur, *l'Internet Protocol Security Standard* fournit une sécurisation au niveau IP. Développé à l'origine le cadre d'IPv6 et adapté à IPv4, IPSec offre les services de contrôle d'accès, d'authentification, d'intégrité et de confidentialité des données, il met en œuvre un mécanisme d'anti-rejeu.

IPSec supporte de nombreux algorithmes de chiffrement (DES, triple DES, RC5, IDEA...), de hachage (MD5, SHA-1...) et d'authentification (signatures RSA ou DSS, clé sécrète, clé publique). Dans ces conditions, l'utilisation d'IPSec est précédée d'une phase de négociation pour déterminer les mécanismes qui seront utilisés. L'ensemble des informations partagées entre les deux systèmes, pour établir une communication sécurisée, constitue une association de sécurité (**SA**, *Security Association*). Une association de sécurité est unidirectionnelle, un échange de données *full duplex* aboutit à la création de deux associations de sécurité.

IPSec intègre deux modes de travail, le **mode transport** et le **mode tunnel** (figure 17.23). Le mode transport ne protège que le champ données du datagramme IP. Le mode tunnel encapsule le datagramme IP d'origine, un nouvel en-tête IP est ainsi ajouté, les adresses IP source et destination initiales sont masquées.

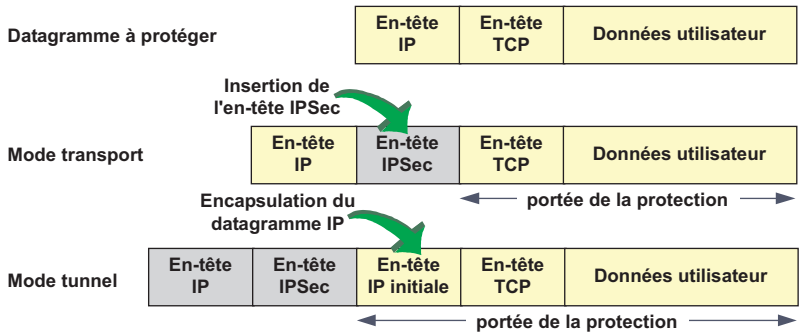


Figure 17.23 IPSec, mode transport et mode tunnel.

L'extension d'authentification (AH)

L'en-tête d'authentification (**AH**, *Authentification Header*) certifie au destinataire du paquet IP l'intégrité des données et l'identité de l'origine. Compte tenu de la modification par les éléments du réseau de certaines données d'en-tête IP (TTL, *Time to Live*...), le *digest* ne porte que sur les données non modifiées par le réseau. Lors du calcul, ces champs sont mis à zéro. L'en-tête AH comporte l'identifiant de l'association de sécurité et, pour éviter le rejeu, un numéro de séquence unique. Les données de l'en-tête AH sont incluses dans le calcul.

L'extension de confidentialité-authentification (ESP)

L'en-tête de confidentialité (**ESP**, *Encapsulating Sécurity Payload header*) garantit la confidentialité des datagrammes, l'intégrité des données et l'identité de la source, il se décompose en trois champs (figure 17.24) :

– à l'instar de l'en-tête AH, le sous-en-tête ESP comprend les données relatives à l'identification de l'association de sécurité et un numéro de séquence « anti-rejeu »,
– un *trailer* (en-queue) ESP précise la portée du chiffrement (mode transport ou mode tunnel),
– un *trailer* d'authentification ESP comporte les données d'authentification.

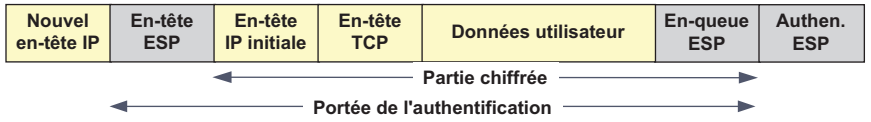


Figure 17.24 L'en-tête ESP en mode tunnel.

17.3.3 La protection du réseau

Les menaces

Les menaces contre les systèmes visent essentiellement à les rendre inaccessibles ou à en altérer profondément les performances. Par exemple, le protocole **ICMP** (*Internet Control Messages Protocol*) constitue l'une des failles (vulnérabilités) des environnements TCP/IP. En effet, il suffit, par exemple, d'adresser à un routeur d'interconnexion des paquets ICMP de

© Dunod – La photocopie non autorisée est un délit

signalisation de congestion pour que le routeur destinataire ralentisse ses émissions de messages vers le réseau extérieur. Cela peut faire supposer à un abonné que le réseau, auquel il a souscrit, n'est pas suffisamment dimensionné.

De même, les paquets ICMP sont utilisés par le protocole RIP (ICMP *redirect*) pour modifier les tables de routage. Il est alors possible de faire croire à un routeur qu'il n'existe plus aucune route pour aller vers tel ou tel site, ou même de détourner le trafic à destination d'un autre site. Ces attaques sont généralement difficiles à détecter.

Les attaques peuvent se classer en deux catégories : celles qui visent à prendre connaissance d'informations soit pour les exploiter soit pour les altérer et celles qui visent à paralyser voire détruire les systèmes. Les modes d'attaque sont nombreux, ils vont de la simple usurpation de mots de passe (*brute force attack*[1] ou *dictionary attack*[2]...) à l'introduction de code malicieux (virus) en passant par la mystification des systèmes (*IP Spoofing*[3]...).

Protection de l'intranet

➤ Protection du réseau local en interne

La sécurisation de la composante locale vise deux objectifs. Le premier tente de prévenir les connexions non autorisées par le contrôle d'adresses (association d'un port du commutateur ou du hub et d'une adresse MAC) et la désactivation des prises non utilisées. Le second assure un cloisonnement des trafics par la constitution de VLAN[4].

➤ Filtrage du trafic par le routeur d'accès

Le moyen le plus simple de protéger le réseau contre les intrusions peut être réalisé avec le routeur d'accès (figure 17.25).

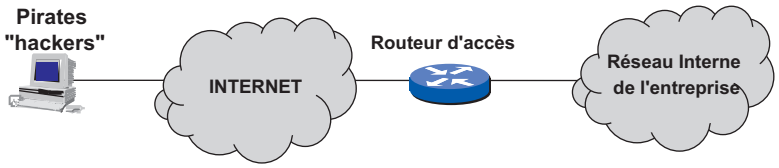


Figure 17.25 Contrôle du trafic par le routeur d'accès.

Le routeur peut assurer des fonctions simples de filtrage par analyse des adresses source et destination. Le routeur n'a de visibilité que sur les données protocolaires du niveau 3, c'est-à-dire les adresses et, dans le mode IP, le protocole transporté dans le datagramme. Ses possibilités de filtre sont donc réduites à ces deux éléments, la sécurité offerte est faible. Les règles de filtrage sont réunies dans des listes (**ACL**, *Access Control List*). La figure 17.26 donne un exemple de règles de filtrage, où « * » signifie toute valeur.

Le filtre de la figure 17.26 n'autorise le trafic qu'entre deux établissements de l'entreprise. L'établissement de filtres est délicat, il nécessite une analyse fine des trafics autorisés et des

1. Tentative de pénétrer un système en essayant toutes les combinaisons possibles de mots de passe.
2. Ces attaques visent à déchiffer les mots de passe encryptés par comparaison avec un dictionnaire de mots de passe chiffrés.
3. IPSpoofing consiste à modifier les adresses IP pour intercepter un trafic.
4. Les VLAN ont été étudiés à la section 12.8.

Action	Protocole	Source	Destination	Commentaire
Accept	*	194.23.10.0/24	194.23.11.0/24	Trafic sortant vers établissement de Paris
Accept	*	194.23.11.0/24	194.23.10.0/24	Trafic entrant de l'établissement de Paris
Rejet	*	*	*	

Figure 17.26 Exemple de règles de filtrage.

trafics interdits. Dans notre exemple simple, l'écriture de la ligne 3 en tête de liste interdirait tout trafic ! Lorsque les filtres sont décrits très finement, il n'est pas rare que certaines lignes soient en contradiction.

➤ La translation d'adresses (RFC 1631)

La translation d'adresse[5] est un moyen de contourner la pénurie d'adresses Internet, mais aussi de masquer le plan d'adressage de l'entreprise (*IP masquerade*).

La traduction statique fait correspondre à une adresse interne du réseau une adresse externe, généralement une adresse publique. Ce mode de translation résout à la fois le problème de la pénurie d'adresse, du masquage du plan d'adressage local (mascarade) et sécurise le réseau en n'autorisant que certaines stations à accéder à l'Internet (figure 17.27).

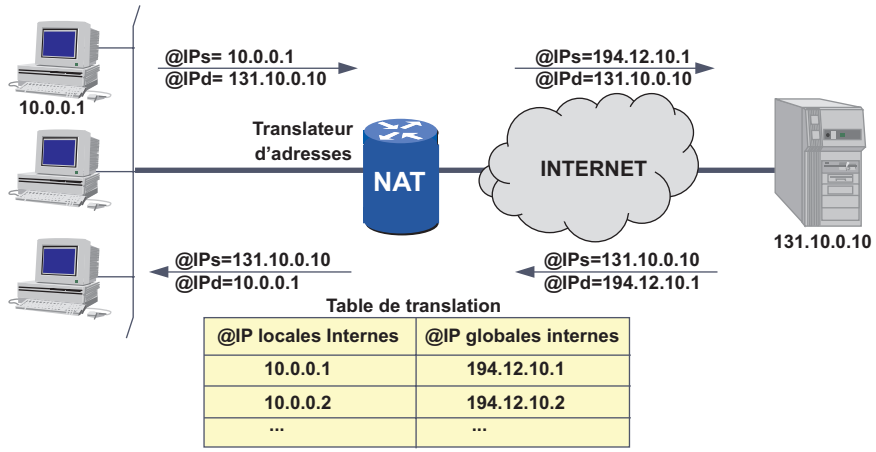


Figure 17.27 Traduction statique d'adresses.

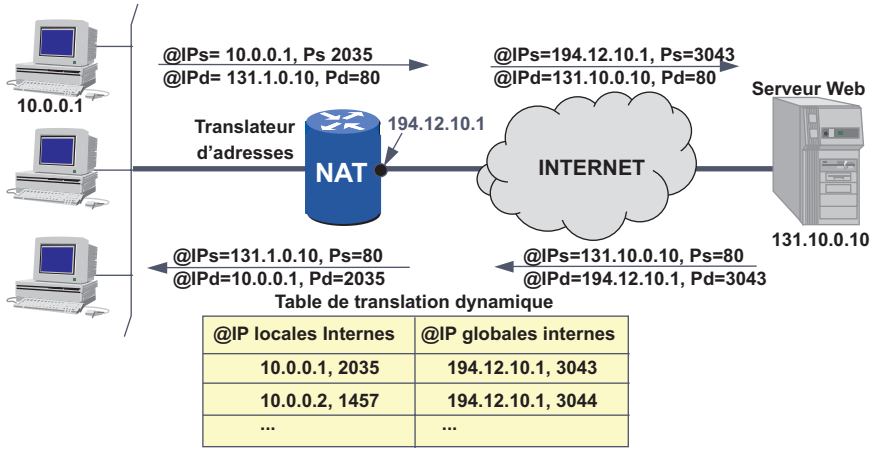
La translation statique limite le nombre de machines ayant accès à l'extérieur au nombre d'adresses publiques attribuées. La traduction dynamique s'affranchit de cette limite. Lorsqu'une machine veut atteindre une machine extérieure, le NAT associe à l'adresse locale interne une adresse globale interne, ou adresse externe, choisie parmi un pool d'adresses mises à sa disposition. Le NAT introduit un protocole à état, indépendamment du fait qu'en cas de défaillance du NAT les relations sont perdues, l'état doit être détruit en fin de communication et l'adresse attribuée rendue disponible pour une autre connexion vers l'extérieur. Un tempori-

5. La notion de translation d'adresses a été introduite à la section 10.2.2.

© Dunod – La photocopie non autorisée est un délit

sateur est donc associé à chaque connexion, il est réinitialisé à chaque message, la connexion est libérée sur *time out*.

Cependant, le nombre d'adresses publiques attribuées peut être insuffisant. Le **NAPT** (*Network Address and Port Translation*) permet à plusieurs machines de partager une même adresse externe par translation du numéro de port (figure 17.28). La fonction dite du **PAT** (*Port Address Translation*) autorise plusieurs milliers de connexion à se partager une même adresse IP externe dite aussi globale interne.



@IP locales Internes	@IP globales internes
10.0.0.1, 2035	194.12.10.1, 3043
10.0.0.2, 1457	194.12.10.1, 3044
...	...

Figure 17.28 Principe de la translation de port.

En translation dynamique, la correspondance @IP interne/@IP externe est initialisée par la machine interne. Un datagramme entrant, sans correspondance dans la table de translation, est rejeté. Pour donner accès, aux machines extérieures, à certains services on peut utiliser la technique dite du « *Port forwarding* » soit pour accéder directement au service concerné, soit en passant par les services d'un **DNS** (*Domain Name System*). La table de translation est prérenseignée de l'adresse du ou des services ouverts (translation statique). La figure 17.29 illustre ce principe dans le cas où seul le DNS est visible de l'extérieur. Lors d'une requête entrante dont le port destination est le port 53 (DNS), le NAT « *forwarde* » la requête au DNS. Il extrait de la réponse du DNS l'adresse de la machine à atteindre (194.12.10.2 dans notre exemple) et initialise une entrée dans la table. Cette technique nécessite une adresse publique par machine visible de l'extérieur.

Si le NAT masque au monde extérieur le plan d'adressage de l'entreprise et protège les machines contre des attaques directes, il est consommateur de ressources et pénalise les performances du réseau. En effet, il nécessite notamment de recalculer les *checksum* (IP et TCP). De plus, il est, en principe, incompatible avec IPSec, du moins en mode tunnel (encapsulation des champs adresses).

➤ Les pare-feu (firewall)

Le pare-feu (*firewall*) est un système aux fonctions de filtrage évoluées. Indépendamment des fonctions de routage et de translation d'adresses, chaque paquet reçu est examiné, une décision de rejet ou d'acceptation est prise en fonction de nombreux critères :

– l'adresse destination,

– l'adresse source,
– le protocole transporté (ICMP, UDP...),
– le port destination,
– le port source
– la valeur de certains flag (ACK, SYN...)...

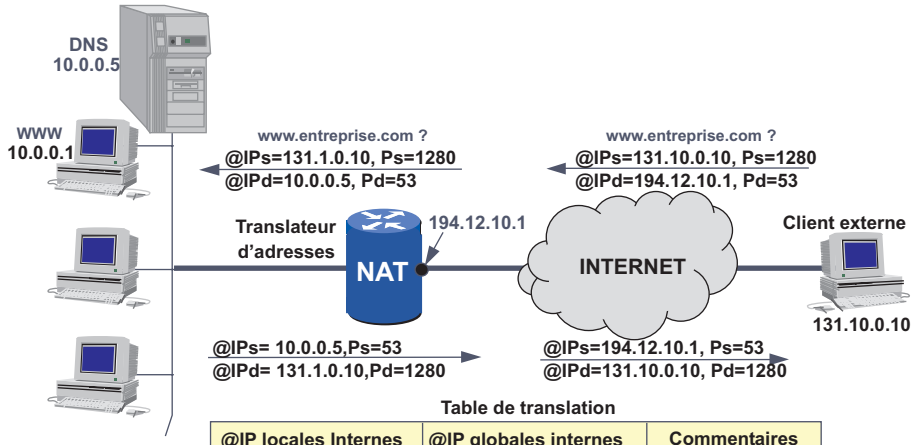


Table de translation

@IP locales Internes	@IP globales internes	Commentaires
10.0.0.5, 53	194.12.10.1, 53	Permanente, DNS
10.0.0.1, 80	194.12.10.2,80	
...	...	

Figure 17.29 Translation d'adresse et trafic entrant.

La décision est prise pour chaque datagramme, il n'y a pas de notion de contexte. Il existe deux types de pare-feu (figure 17.30).

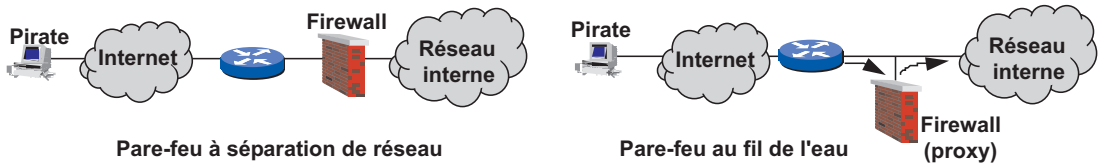


Figure 17.30 Les différents modes d'utilisation des pare-feu (*firewall*).

Le pare-feu à séparation des réseaux segmente le réseau en deux tronçons : le réseau interne et le réseau externe. Il contrôle le trafic et peut réaliser une translation d'adresses (NAT). Le pare-feu au fil de l'eau n'effectue aucune séparation physique des réseaux. Cependant, comme le pare-feu à séparation des réseaux, il réalise l'isolation des trafics. Les postes ne communiquent qu'avec le pare-feu (passerelle par défaut) et le routeur ne voit que le pare-feu[6].

La figure 17.31 illustre les différentes architectures de sécurité envisageables, la mise à disposition d'un serveur public (service Web, messagerie...) est généralement réalisée par la constitution d'une zone de sécurité dite **DMZ** (*DeMilitarized Zone*). Différentes zones de sécu-

6. Un pare-feu au fil de l'eau est généralement désigné sous le terme de bastion ou proxy.

© Dunod – La photocopie non autorisée est un délit

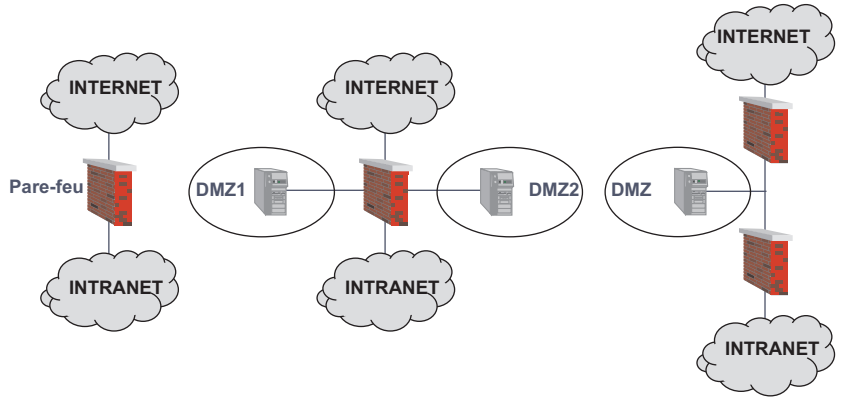


Figure 17.31 Les différentes architectures de sécurité.

rité peuvent être constituées, chacune accessible selon des critères spécifiques (filtres). L'utilisation de deux pare-feu permet de renforcer cette sécurité. Le premier masque, aux pirates éventuels, le second. En choisissant les deux pare-feu de marque différente, on améliore encore la sécurité, les vulnérabilités ou failles de l'un étant différentes de celles de l'autre. La zone démilitarisée accueillera les différents serveurs accessibles à la fois par le personnel de l'entreprise et par le monde extérieur. Pour différencier les services offerts et les règles de filtrage, il est possible de définir plusieurs DMZ, dans ce cas généralement l'une est accessible à tous, et l'autre aux personnels de l'entreprise.

La définition des filtres est similaire à celle réalisée pour les routeurs, seule, la portée de l'analyse est plus profonde. Tout datagramme non autorisé est rejeté. En cas de tentative de violation d'une règle, les pare-feu émettent des alertes. Un fichier (logs) conserve une trace de tous les événements. La figure 17.32 présente quelques exemples de règles de filtrage.

Règles	Destination		Source		Flag	Action	Commentaire
	Adresse	Port	Adresse	Port			
1	Externe	25	Interne	>1023		accept	Connexion vers serveurs SMTP
2	Interne	>1023	Externe	25	ACK	accept	Réponses aux connexions SMTP
3	Externe	23	Interne	>1023		accept	Connexion à des services Telnet
4	10.0.0.5	23	194.28.12.1	>1023		accept	Station externe autorisée Telnet
5	194.28.12.1	>1023	10.0.0.5	23		accept	Trafic Telnet station 194.28.12.1
6	Interne	23	Externe	>1023	ACK	accept	Réponses au trafic Telnet

Figure 17.32 Exemples de règles de filtrage.

L'énoncé des règles 1 et 2 autorise le trafic de toutes les stations du réseau interne vers des serveurs SMTP externes, mais n'autorise pas les connexions d'origine externe en provenance d'un service sur le port 25 puisque les messages d'origine externe doivent avoir le bit ACK

(TCP) positionné, de même pour les règles 2 et 6. Cependant, pour autoriser une station spécifique à ouvrir depuis l'extérieur une session Telnet, nous avons inséré les règles 4 et 5. Si celles-ci avaient été placées après la règle 6, aucune connexion en provenance de l'extérieur à destination d'un service Telnet interne n'était autorisée (bit ACK)

➤ Les passerelles applicatives

Les passerelles applicatives (*Application Layer Gateway* ou *Proxy-Server*) établissent une double connexion (figure 17.33). Le filtrage s'effectue alors au niveau de chaque service offert. Les services internes sont invisibles de l'extérieur. La passerelle peut réaliser des conversions de protocoles (messagerie...).

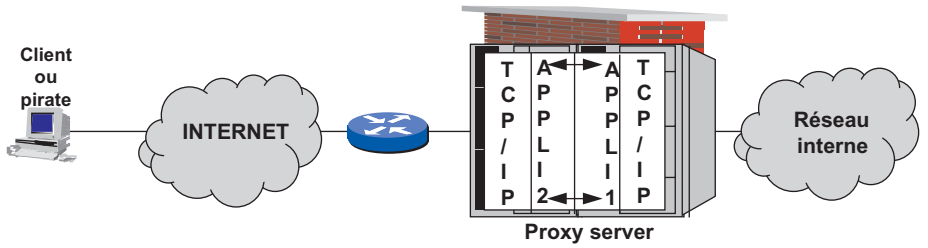


Figure 17.33 Le filtrage par un proxy-server.

Les passerelles applicatives, à l'instar des pare-feu, mémorisent toutes les connexions et peuvent en éditer la liste. L'association pare-feu à séparation de réseau et proxy-server (pare-feu au fil de l'eau) constitue une protection efficace contre les intrusions. Mais quels que soient les moyens mis en œuvre, les virus et chevaux de Troie restent indécelables.

➤ Les codes malicieux (virus)

Un virus est un programme « parasite » qui s'attache à un programme principal dont il modifie l'environnement de travail avec un objectif généralement destructeur. Les programmes virus ont aussi la possibilité de se propager de machine en machine directement avec le programme infecté (copie de programme), mais aujourd'hui de plus en plus par exploitation du carnet d'adresses de la machine infectée.

Les virus fonctionnent en tâche fond. Lorsqu'une certaine activité est réalisée le virus effectue la tâche pour laquelle il a été programmé. Les virus peuvent altérer les données, les diffuser vers des adresses aléatoires ou préprogrammées, modifier le comportement du système allant de l'instabilité à la paralysie voire à la destruction de certains composants du système (effacement du bios...).

Des logiciels dit antivirus permettent de se protéger des virus connus. Cependant, malgré les mises à jour, les « pirates » ont toujours un virus d'avance. La seule parade efficace consiste à n'échanger des données avec personne et de ne jamais raccorder son ordinateur à un réseau !

Protection des accès, les VPN

Autoriser à des utilisateurs nomades l'accès au système d'information de l'entreprise nécessite la mise en œuvre d'un système d'accès distant (**RAS**, *Remote Access Service*) qui garantisse

© Dunod – La photocopie non autorisée est un délit

l'authentification et la confidentialité des données. La figure 17.34 illustre les différents modes d'accès aux réseaux d'une entreprise.

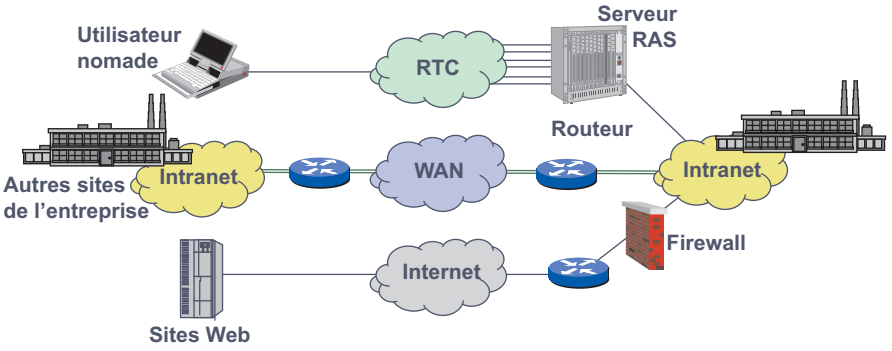


Figure 17.34 Les différents accès possibles au réseau d'une entreprise.

Cette approche traditionnelle en multipliant les modes d'accès complexifie la maintenance du système et, en terme, de sécurité le fragilise. Les **VPN** (*Virtual Private Network*) en unifiant les technologies d'accès et en sécurisant les données apportent une solution aux problèmes précédents. Un VPN correspond à la réalisation dans un réseau public de tunnels chiffrés simulant ainsi un réseau privé de liaisons point à point. La figure 17.35 illustre l'évolution du réseau de la figure 17.34 vers un VPN. Le service de VPN peut être offert par un opérateur (Telcos) ou réalisé à travers Internet.

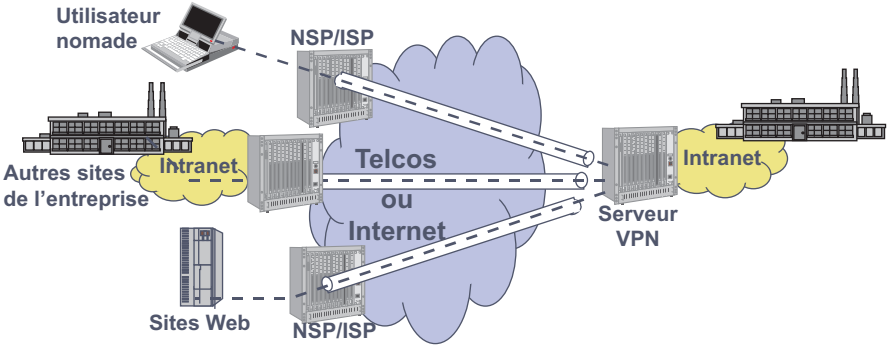


Figure 17.35 Évolution du réseau vers le VPN.

Réaliser un tunnel consiste à assurer le transport des données utilisateur dans un protocole qui masque ces dernières (encapsulation). Selon que ce soit le terminal client où l'opérateur qui initialise le tunnel, le tunnel est dit tunnel client ou tunnel opérateur.

Le tunnel opérateur est initialisé par l'opérateur (figure 17.36), le client se connecte de façon transparente. Avant d'établir le tunnel vers l'entreprise, l'opérateur (ISP) identifie et authentifie le client. Si l'utilisateur est reconnu, l'ISP ouvre un tunnel vers l'entreprise qui, de même, authentifie le client avant d'accepter la connexion. Lorsque le tunnel est initialisé par le client (tunnel client ou de bout en bout), celui-ci doit être doté d'un logiciel spécifique (figure 17.37). Selon le niveau de l'encapsulation on distingue des tunnels de niveau 2 ou 3 (IPSec[7]). Trois protocoles permettent de réaliser des tunnels de niveau 2 :

7. Les tunnels de niveau 3 de type IPSec ont été étudiés à la section 17.3.2.

– **L2F**, *Layer 2 Forwarding*, d'origine Cisco est un tunnel dit opérateur, il est initialisé par le fournisseur d'accès (**ISP**, *Internet Service Provider*) et se termine chez le client par un équipement spécifique. Le protocole L2F n'assure l'authentification de l'utilisateur qu'à la connexion. Le tunnel L2F ne garantit pas la confidentialité des données (pas de chiffrement). Cependant, un chiffrement utilisateur de bout en bout peut être mis en œuvre.

– **PPTP**, *Point-to-Point Tunneling Protocol*, d'origine Microsoft est une technique de tunnel de bout en bout (le tunnel est initialisé par le client). La session client PPP est transportée de bout en bout dans une encapsulation spécifique (**GRE**, *Generic Routing Encapsulation*). Les datagrammes peuvent être chiffrés par le protocole d'origine Microsoft **MPPC** (*Microsoft Point-to-Point Encryption*).

– **L2TP**, *Layer 2 Tunneling Protocol*, d'origine IETF, L2TP est un protocole de tunnel opérateur (ouvert par le *provider*), il autorise les appels *outbounds* (appels initiés depuis l'intranet destination), il peut être utilisé conjointement à IPSec pour chiffrer les données, en-tête IP d'origine comprise.

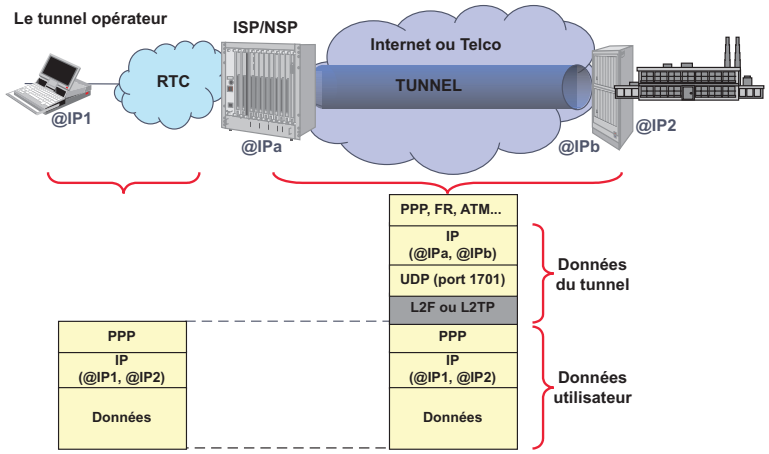


Figure 17.36 Tunnel opérateur (L2F, L2TP).

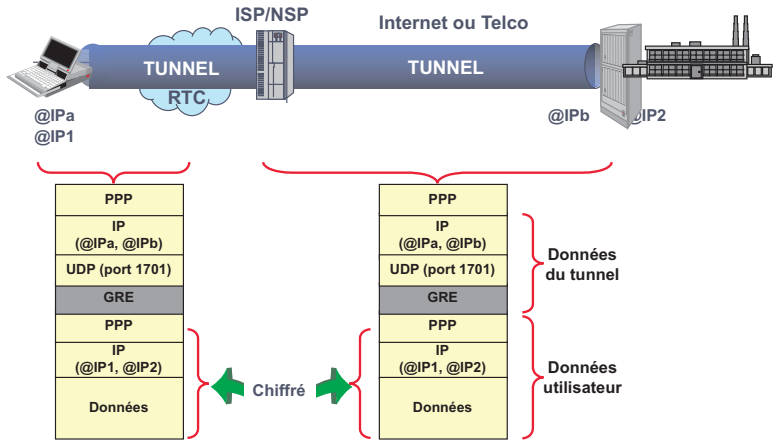


Figure 17.37 Tunnel client (PPTP).

© Dunod – La photocopie non autorisée est un délit

17.4 LE COMMERCE ÉLECTRONIQUE

Le problème essentiel du commerce électronique consiste à garantir la sécurité des transactions (authentification des interlocuteurs, confidentialité des échanges, sécurité bancaire...). Deux approches du commerce électronique sont envisageables selon que l'organisme bancaire participe directement à la transaction (paiement *on-line*) où que l'organisme bancaire est étranger à la transaction (paiement *off-line*).

17.4.1 Le paiement off-line (ecash)

Dans ce mode de paiement, le client approvisionne un compte local en monnaie électronique (monnaie virtuelle) et réalise la transaction commerciale avec elle. La figure 17.38 illustre ce principe.

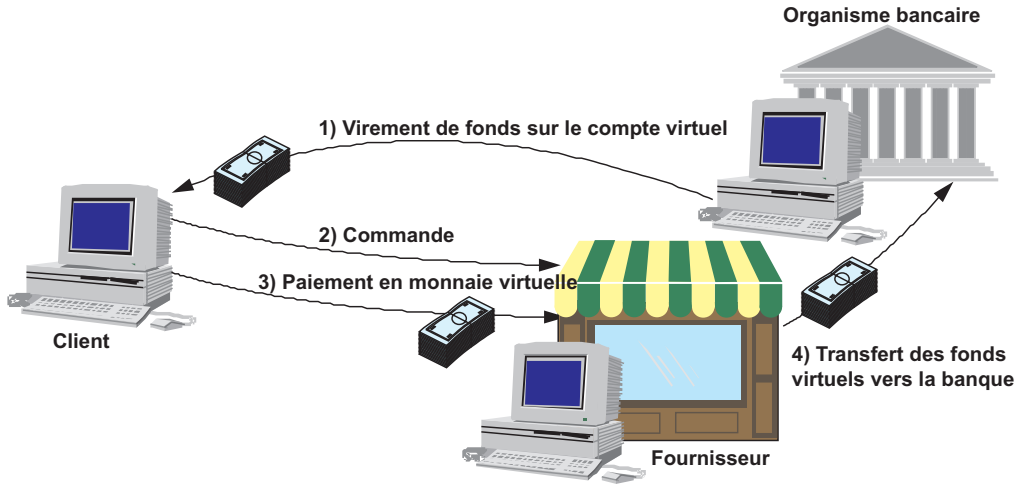


Figure 17.38 Le paiement *off-line*.

17.4.2 Le paiement on-line

Dans ce type de relation, le paiement s'effectue à l'aide d'une carte bancaire. Le client joint à son bon de commande (crypté avec la clé publique du vendeur) son numéro de carte bancaire (crypté avec la clé publique de la banque). Le vendeur transmet à la banque le numéro de carte crypté et le montant de l'achat. La banque effectue le transfert de fonds (figure 17.39)

Cette approche (**SET**, *Secure Electronic Transaction*) est retenue par la plupart des organismes de cartes de crédit (Visa, Mastercard, American Express...) et les constructeurs comme Microsoft, Netscape et IBM.

Cependant, elle présente l'inconvénient de multiples transferts de clés entre le vendeur, le client et les banques. Le protocole **JEPI** (*Joint Electronic Payment Initiative*), défendu par le World Wide Web Consortium et Commerce Net, vise à minimiser les échanges et à permettre les petits paiements.

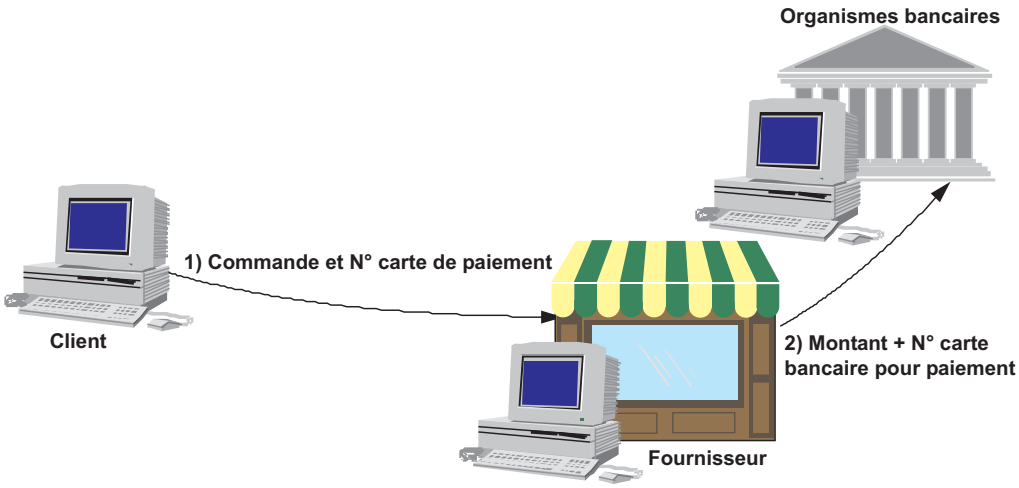


Figure 17.39 Principe du paiement *on-line*.

17.5 CONCLUSION

Quels que soient les moyens mis en œuvre, du fait de l'ouverture vers l'extérieur, les réseaux seront de plus en plus vulnérables. Dans ses conditions, il appartient à chaque entreprise de mesurer le risque et le coût d'une indisponibilité de leur système, de la divulgation d'information... et déterminer une politique dite de sécurité, d'en mesurer les coûts et d'assurer en permanence une veille technologique pour que les moyens employés restent efficaces devant l'évolution des menaces.

© Dunod – La photocopie non autorisée est un délit

EXERCICES

Exercice 17.1 MTTR/MTBF

Soient deux systèmes informatiques identiques interconnectés via les services d'un opérateur et une liaison téléphonique de secours (figure 17.40). Quel est, pour l'ensemble du système, la disponibilité, l'indisponibilité et la MTBF du système, compte tenu des éléments ci-dessous (par hypothèse, on admettra que la MTBF de l'opérateur inclut la liaison d'abonné et les modems d'extrémité) ?

	MTBF	MTTR
Système 1	4 mois	8 heures
Système 2	4 mois	8 heures
Modem	2 ans	5 heures
RTC	2 ans	24 heures
Telcos	2 ans	2 heures

On considérera qu'un mois représente 200 heures et une année 2 400 heures

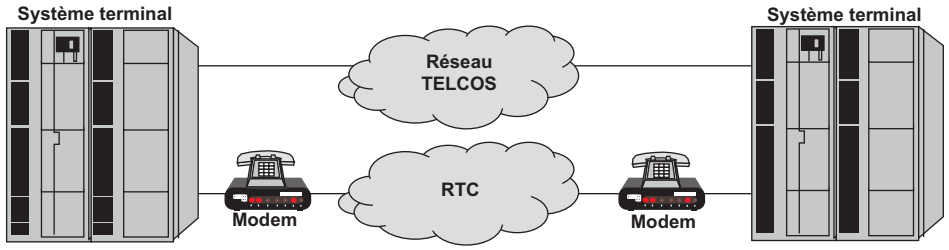


Figure 17.40 Système avec ligne de secours.

Exercice 17.2 Systèmes à clés symétriques ou secrètes

Un système de messagerie sécurisé met en relation *N* utilisateurs. Dans un système à clés secrètes, chaque utilisateur doit, pour communiquer avec les autres abonnés, connaître la clé secrète de chacun des autres abonnés aux systèmes. En supposant, l'administration des clés centralisée, on vous demande de déterminer le nombre de clés que le système devra gérer. Que devient ce nombre dans un système à clés publiques ?

Exercice 17.3 Algorithme à translation de César

Retrouver le clair du message codé à l'aide de l'algorithme de César « HTIFLJIJHJXFW ».

Exercice 17.4 Algorithme de substitution de Vigenère

Le système de Vigenère utilise la substitution polyalphabétique. Son principe est relativement simple. Dans un tableau, dit carré de Vigenère, on remplace la lettre du message à chiffrer par la lettre obtenue à l'intersection de la colonne repérée par cette lettre, et de la ligne définie par la lettre de la clé associée à la lettre du message.

Soit, par exemple à coder le message « ABACADRABRA » à l'aide de la clé « CLE ».

Méthode :

a) Supprimer tous les blancs du message d'origine.

b) Recopier autant de fois que nécessaire la clé. Afin d'obtenir un texte de longueur identique à celle du message.

c) Déterminer la lettre du cryptogramme en pratiquant comme suit :

– la lettre du cryptogramme est la lettre obtenue à l'intersection de la colonne de la lettre sélectionnée dans le message et de la ligne déterminée par la lettre en correspondance dans le texte (clé).

Clair →	A	B	A	C	A	D	R	A	B	R	A
Clé →	C	L	E	C	L	E	C	L	E	C	L

La lettre D du message est en correspondance avec la lettre E de la clé, elle sera codée par la lettre obtenue à l'interception de la colonne D et de la ligne E soit H (figure 17.41).

		1	2	3	↓ 4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	1	A	B	C	***D***	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	2	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K	R	S	T	U	V	W	X	Y	Z	A
	3	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	4	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
→	5	***E***	F	G	**H**	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	6	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	7	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	B	E	F
	8	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y	Y	Z	A	B	C	D	E	F	G
	9	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	10	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	11	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	12	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	13	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	14	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	15	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	16	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	17	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	18	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K
	19	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K	R
	20	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	21	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	22	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	23	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K	R	S	T	U	V
	24	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	25	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	26	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 17.41 Carré de Vigenère.

Retrouver le clair du crypte « LEDCITMHGMMZWRGII » codé à l'aide de la clé « SECRET ».

© Dunod – La photocopie non autorisée est un délit

Exercice 17.5 Systèmes à clés asymétriques

Le système de cryptographie à clé asymétrique le plus répandu, le RSA, repose sur l'arithmétique des grands nombres. La fonction de chiffrement est de la forme :

$$\text{Crypte} = \text{Clair}^{\text{clé C}} \text{ modulo } n$$

Crypte : le message codé — Clair : message à coder

clé C : clé de chiffrement — n : produit de nombres premiers.

La fonction de déchiffrement est identique :

$$\text{Clair} = \text{Crypte}^{\text{clé D}} \text{ modulo } n$$

Crypte : le message codé — Clair : message à coder

clé D : clé de déchiffrement — n : un produit de nombre premier.

L'algorithme de détermination des clés est rappelé ci-dessous :

1) Choisir deux nombres premiers p et q grands et différents ($> 10^{100}$).
2) Calculer n tel que $n = p \cdot q$.
3) Choisir les clés telles que $C \cdot D = 1 + M\,[(p - 1) \cdot (q - 1)]$, où M est un entier qui satisfasse l'égalité.
4) Définir la longueur maximale (L) du bloc de bits sur lequel on applique l'opération de sorte que $2^L < n$.

On vous demande :

a) Calculez les plus petites clés possibles (pour des raisons tenant aux possibilités de calcul p et q seront choisis les plus petits possibles). Pour ces clés et pour toutes les valeurs (fonction de L) que peuvent prendre les messages clairs, établissez la matrice de codage et de décodage en renseignant le tableau ci-dessous.

Clair	N = Clair ^{C}	Crypte = N mod n	N = Crypte ^{D}	Clair = N mod n

b) Est-il possible d'utiliser cette combinaison de clés pour transmettre un message chiffré ? Expliquez pourquoi et indiquez la ou les condition(s) supplémentaire(s) à introduire dans l'algorithme.

c) Compte tenu de la question précédente, déterminez les plus petites clés utilisables et établissez la matrice de codage et de décodage.

d) On désire envoyer le message clair « MODEM » codé en ASCII sur 8 bits (le bit de poids fort est positionné à zéro), déterminer le crypte.

Exercice 17.6 Système de Diffie-Hellman

Déterminer la clé de session Diffie-Hellman, si Alice communique à Bob les nombres g = 3 et n = 23. Sachant qu'Alice tire le nombre aléatoire A = 5 et Bob le nombre B = 7 ?

Chapitre **18**

Administration des réseaux

18.1 GÉNÉRALITÉS

18.1.1 Définition

La stratégie générale d'une entreprise résulte de nombreux facteurs tant internes qu'externes. Mais, indépendamment de la compétence de ses décideurs, la pertinence du système d'information et les moyens d'y accéder sont parmi les éléments majeurs du système décisionnaire.

Dans ces conditions, le système de communication, dont la matérialisation est le réseau télécom de l'entreprise, devient un enjeu stratégique. L'ensemble des moyens mis en œuvre, pour garantir l'efficacité du système et sa disponibilité, pour assurer la surveillance des coûts et la planification des évolutions constitue l'administration de réseau (*Network Management*).

18.1.2 Principe général

L'administration d'un réseau suppose l'existence d'un système d'information décrivant le réseau de l'entreprise et recensant toutes les données et événements relatifs à chaque constituant du réseau administré (figure 18.1).

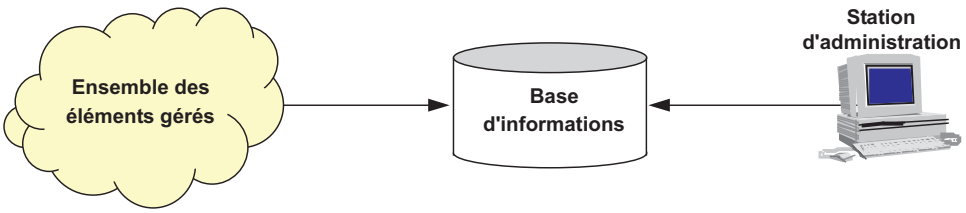


Figure 18.1 Principe général d'un système d'administration réseau.

Le traitement des informations collectées appartient à la sphère de compétence de l'administrateur. L'expérience et l'intuition, qualités essentielles de ce dernier, ne sont pas modélisables, cependant, aujourd'hui, les moteurs d'inférence (intelligence artificielle) constituent une aide non négligeable au diagnostic, à la simulation et à la planification des opérations correctives ou évolutives.

18.1.3 Structure d'un système d'administration

Un système réseau comporte un grand nombre de composants (objets) que le système d'administration surveille. Dans chaque objet, un programme en tâche de fond (*daemon*) transmet régulièrement, ou sur sollicitation, les informations relatives à son état (figure 18.2).

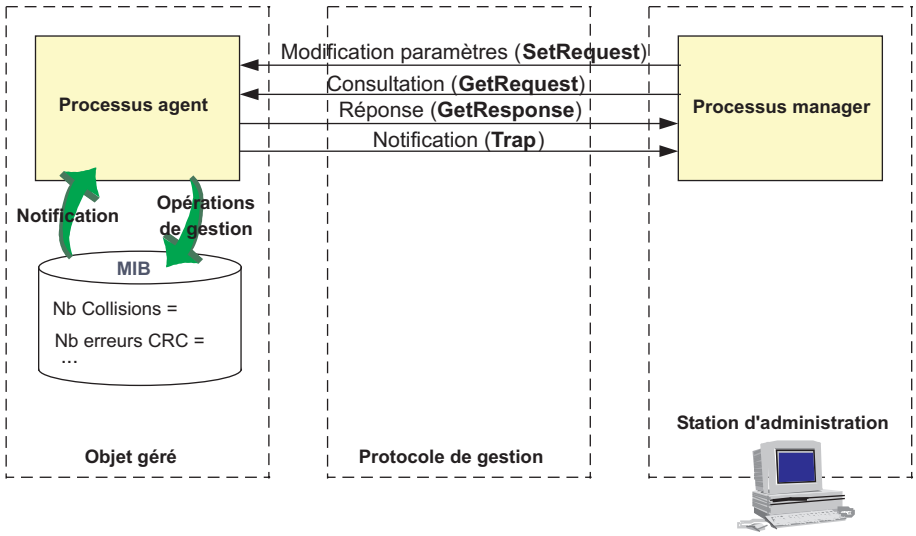


Figure 18.2 Structure fonctionnelle d'un système d'administration.

Les échanges s'effectuent à deux niveaux : entre le composant administré (*processus agent*) et sa base d'information (**MIB**, *Management Information Base*) d'une part, et d'autre part, entre le composant et le programme d'administration (*processus manager*).

18.2 L'ADMINISTRATION VUE PAR L'ISO

18.2.1 Généralités

L'ISO ne spécifie aucun système d'administration de réseau, elle définit un cadre architectural général (ISO 7498-4, *OSI Management Framework*) et un aperçu général des opérations de gestion des systèmes (ISO 10040, *OSI System Management*). Ces documents de base décrivent trois modèles :

– un modèle organisationnel ou architectural (**MSA**, *Managed System and Agents*) qui organise la gestion OSI et définit la notion de systèmes gérés et gérants (**DMAP**, *Distributed Management Application Processus*) ;

– le modèle informationnel (**MIB**, *Management Information Base*) qui constitue la base de données des informations de gestion. La MIB énumère les objets gérés et les informations s'y rapportant (attributs) ;
– le modèle fonctionnel (**SMFA**, *Specific Management Function Area*) qui répartit les fonctions d'administration en 5 domaines (aires) fonctionnels (figure 18.3).

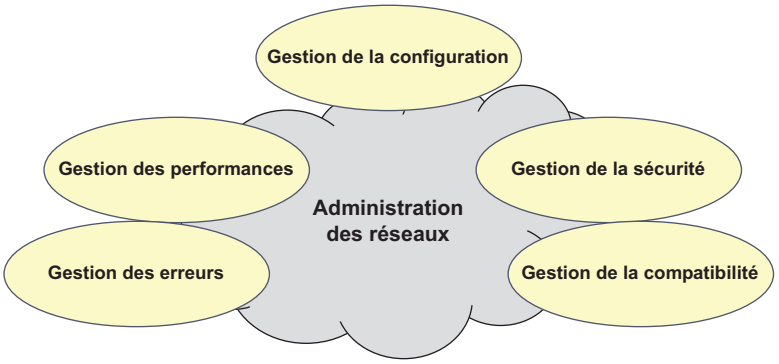


Figure 18.3 Les aires fonctionnelles de la gestion ISO.

18.2.2 Les différents modèles

Le modèle architectural

Le modèle architectural définit trois types d'activité : la gestion du système (*System Management*), la gestion de couche (*Layer management*) et les opérations de couche (*Layer Operation*).

La gestion du système (**SMAE**, *System Management Application Entity*) met en relation deux processus : un **processus gérant** et un **processus agent**. L'agent gère localement un ensemble de ressources locales (équipements, protocoles...) sous le contrôle de l'agent gérant (figure 18.4).

La gestion système repose sur des échanges verticaux entre couches (**CMIS**, *Common Management Information Service*). CMIS (ISO 9595) définit les primitives d'accès aux informations. Ces primitives assurent le transfert d'information vers les applications de gestion (**SMAP**, *System Management Application Process*) non spécifiées par l'ISO.

La gestion de couche, ou protocole de gestion de couche, fournit les moyens de transfert des informations de gestion entre les sites administrés, c'est un dialogue horizontal (**CMIP**, *Common Management Information Protocol*, ISO 9596). Les opérations de couche (*N*), ou protocole de couche (*N*), supervisent une connexion de niveau *N*. Ces opérations utilisent les protocoles OSI classiques pour le transfert d'information.

CMIP utilise les primitives de service suivantes (**CMISE**, *Common Management Information Service Element*) :

– **Get**, cet élément de service est utilisé par le gérant pour lire la valeur d'un attribut ;
– **Set** fixe la valeur d'un attribut ;
– **Event** permet à un agent de signaler un événement ;

© Dunod – La photocopie non autorisée est un délit

– **Create** génère un nouvel objet ;
– **Delete** permet à l'agent de supprimer un objet.

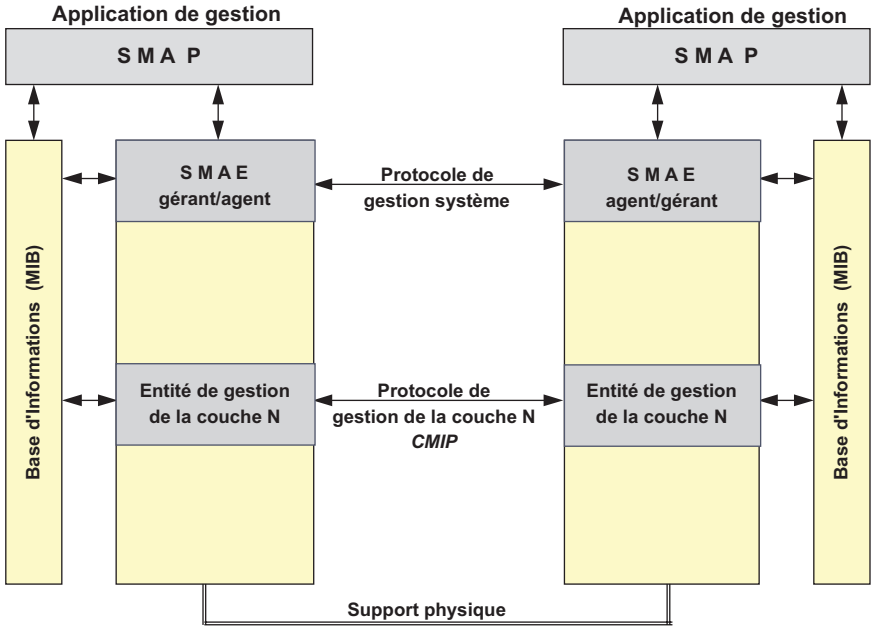


Figure 18.4 Le modèle architectural de l'ISO.

Le modèle informationnel

Le standard OSI décrit une méthode de définition des données d'administration qui modélise la représentation des informations et qui fournit un ensemble de directives pour garantir la cohérence de la base (**SMI**, *Structure of Management Information*).

La représentation des éléments gérés (objets gérés) est orientée objet, les classes et occurrences d'objets sont représentées selon un arbre. Les classes sont rattachées à un arbre dit d'héritage (*Inheritance Tree*), les occurrences d'objets à un arbre dit de contenance (*Containment Tree*). Un objet est décrit par sa classe d'appartenance, son nom, ses attributs et les types d'opération qu'il supporte.

L'ensemble des objets gérés constitue la MIB (ISO 10165). La MIB contient toutes les informations administratives sur les objets gérés (ponts, routeurs, cartes...). La norme ne spécifie aucune organisation particulière des données. Celles-ci peuvent y être organisées selon une structure en ligne, une base de données... Seul, le *processus agent* a accès à la MIB. Le *processus manager* accède aux données via le processus agent.

Le modèle fonctionnel

Ce modèle, plus concret que les précédents, définit des domaines fonctionnels d'administration et leurs relations. Cinq domaines ou fonctions (aires fonctionnelles) y sont décrits (**SMFA**, *Specific Management Function Area*).

➤ Gestion des anomalies

La gestion des anomalies (*Fault Management*) est une fonction dominante. En effet, l'objectif essentiel d'une administration de réseaux est l'optimisation des ressources et des moyens. Il importe donc d'être en mesure de diagnostiquer rapidement toute défaillance du système, que celle-ci soit d'origine externe (ex : coupure d'un lien public) ou interne au système (ex : panne d'un routeur). La gestion des anomalies comporte notamment :

– la surveillance des alarmes (filtre, report...),
– le traitement de celles-ci,
– la localisation et le diagnostic des incidents,
– la mémorisation des anomalies (journalisation),
– la définition des opérations curatives...

➤ Gestion de la comptabilité

La gestion des éléments comptables (*Accounting Management*) permet d'évaluer les coûts et de les imputer aux utilisateurs selon l'usage réel des moyens. Ces informations autorisent la répartition des coûts selon les centres de frais de l'entreprise (comptabilité analytique). La comptabilité comporte les tâches suivantes :

– définition des centres de coût,
– mesure des dépenses de structure (coûts fixes) et répartition,
– mesure des consommations par service,
– imputation des coûts.

➤ Gestion de la configuration et des noms

La gestion de la configuration (*Configuration Management*) consiste à maintenir un inventaire précis des ressources matérielles (type, équipement...) et logicielles (version, fonctions...) et d'en préciser la localisation géographique. La gestion de la configuration associe, à chaque objet géré (chaque objet de l'inventaire), un nom qui l'identifie de manière unique.

➤ Gestion des performances

La gestion des performances (*Performance Management*) met en œuvre les moyens qui permettent d'évaluer le comportement des objets gérés. L'évaluation des performances nécessite la collecte d'informations statistiques afin de déterminer, en permanence, si le réseau est apte à satisfaire les besoins de communication des utilisateurs. La mesure de la dégradation des performances permet d'anticiper les défaillances et de programmer les évolutions du système. La gestion des performances comprend notamment :

– la collecte d'informations (mesure du trafic, temps de réponse, taux d'erreur...),
– le stockage (archivage...),
– l'interprétation des mesures (calculs de charge du système...).

La gestion des performances nécessite de disposer d'outil de modélisation et de simulation pour évaluer l'impact d'une modification de l'un des paramètres du système.

© Dunod – La photocopie non autorisée est un délit

➤ Gestion de la sécurité

La gestion de la sécurité (*Security Management*) couvre tous les domaines de la sécurité afin d'assurer l'intégrité des informations traitées et des objets administrés. L'ISO a défini cinq services de sécurité :

– les contrôles d'accès au réseau,
– la confidentialité (les données ne sont communiquées qu'aux personnes, ou processus autorisés),
– l'intégrité (les données n'ont pas été accidentellement ou volontairement modifiées ou détruites),
– l'authentification (l'entité participant à la communication est bien celle déclarée),
– le non-désaveu (impossibilité pour une entité de nier d'avoir participé à une transaction).

Pour cela l'ISO utilise les mécanismes d'encryptage, l'authentification des extrémités (source et destinataire) et le contrôle des accès aux données (voir chapitre 17).

18.3 L'ADMINISTRATION DANS L'ENVIRONNEMENT TCP/IP

18.3.1 Principes généraux

Standard de fait dans l'administration des réseaux TCP/IP, le protocole **SNMP** (*Simple Network Management Protocol*) est proche des concepts ISO. Cependant, non orienté objet SNMP confond la notion d'attribut et d'objet. Issu du protocole de gestion des passerelles IP (**SGMP**, *Simple Gateway Monitoring Protocol* – RFC 1028), SNMP est décrit dans la RFC 1157. Ce document est complété par de nombreuses RFC dont :

– RFC 1155 qui spécifie comment les objets gérés sont représentés dans les bases d'informations (**SMI**, *Structure of Management Information*). SMI utilise la notation ASN1 (*Abstract Syntax Notation 1*) ;
– les RFC 1156 et 1213 qui définissent les MIB (MIB I et MIB II). Les MIB décrivent les objets gérés (attributs ISO). Une MIB particulière (**RMON MIB**, *Remote Monitor Network MIB*) est spécifiée pour les réseaux locaux (Ethernet et Token Ring), les objets RMON sont implémentés dans des sondes d'analyse et de surveillance. Cependant en environnement commuté, les sondes RMON n'ont accès qu'aux segments sur lesquels elles sont installées. Pour assurer un accès aux différents éléments des réseaux commutés, une sonde spécifique a été définie (RFC 2613, **SMON**, *Switched RMON*).

SNMP spécifie les échanges entre la station d'administration et l'agent. S'appuyant sur UDP (*User Datagram Protocol*), SNMP est en mode non connecté. De ce fait, les alarmes (*trap*) ne sont pas confirmées. La plus grande résistance aux défaillances d'un réseau d'un protocole en mode datagrammes vis-à-vis d'un protocole en mode connecté ainsi que la rapidité des échanges justifient le choix d'UDP. La figure 18.5 illustre les échanges SNMP. Les messages SNMP permettent de lire la valeur (exemple : compteur de collisions) d'un objet administré (attribut d'ISO) (**GetRequest** et **GetNextRequest**), de modifier la valeur d'un objet (**SetRequest**). L'agent administré répond à ces sollicitations par le message **GetResponse**.

Le message **Trap** est émis sur l'initiative de l'agent qui notifie ainsi, à l'administrateur, qu'une condition d'alarme a été détectée.

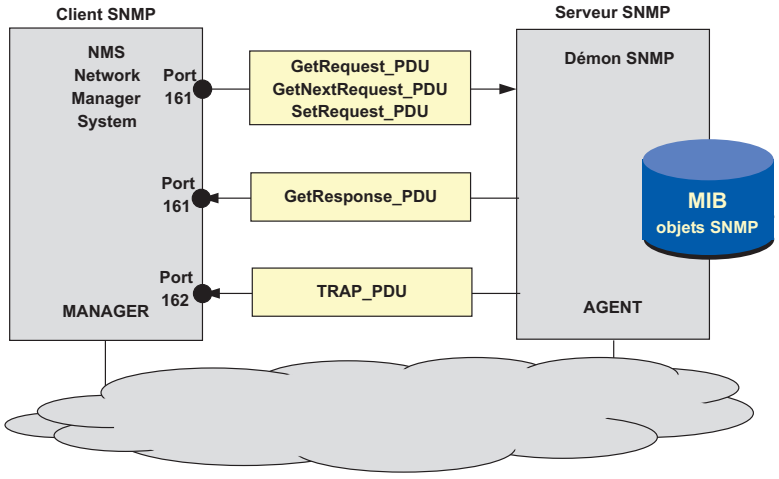


Figure 18.5 Les divers échanges SNMP.

18.3.2 Les MIB

Description des objets

Les MIB décrivent les objets gérés, en définissent le nommage, ils en précisent le type, le format et les actions. Les différentes valeurs des objets ne sont pas contenues dans la MIB, mais dans des registres externes que l'agent vient consulter à la demande du manager. La RFC 1213 (MIB II) formalise une structure de définition des objets.

Ainsi, l'objet **SysUpTime** qui mesure le temps, en centième de seconde, depuis que l'agent a été réinitialisé, est de type *TimeTicks* (type de variable défini dans la SMI, *TimeTicks* mesure le temps en centièmes de seconde) et est accessible uniquement en lecture (*read_only*). Cet objet obligatoire (*mandatory*) est le troisième objet décrit dans la MIB system. Sa description est donnée figure 18.6.

```
OBJECT_TYPE MACRO ::=
BEGIN
  TYPE NOTATION ::=
          "SYNTAX" type (TYPE ObjectSyntax)
          "ACCESS" Access
          "STATUS" Status
  VALUE NOTATION ::= value (VALUE ObjectName)
  DESCRIPTION value (description DisplayString) | empty
  Access ::= "read_only" | "write_only" | "not_accessible"
  Status ::= "madatory" | "optional" | "obsolete" | "deprecated"
  DisplayString ::= OCTET STRING SIZE (0..255)
END
```

Description formelle d'un objet

```
SysUpTime OBJECT_TYPE
  Syntax TimeTicks
  Access read_only
  Status mandatory
  Description "The Time (in hundreths of a
  second) since the network management
  portion of a system was last reinitialized"
::= {system 3}
```

Exemple : description de l'objet SysUpTime

Figure 18.6 Description d'objet selon la MIB II.

© Dunod – La photocopie non autorisée est un délit

Nommage des objets

Les objets (variables) gérés par les MIB sont désignés selon une hiérarchie définie par l'ISO selon un arbre dit **arbre de nommage**. Dans l'arbre de la figure 18.7, chaque organisation de normalisation possède une entrée au premier niveau. Les différentes branches permettent de nommer un objet de manière unique. Les MIB standard établies par l'IETF appartiennent à la branche « internet » et sont classées dans la sous-branche mgmt(2). Ainsi, l'objet *SysUpTime* de la figure 18.7 est désigné par :

iso.org.dod.internet.mgmt.mib - 2.system.sysuptime

Le même objet peut être décrit par le chemin qui de la racine (*root*) mène à l'objet, soit la suite de nombre : **1.3.6.1.2.1.1.3** ou encore plus simplement **mib-2(1.3)**.

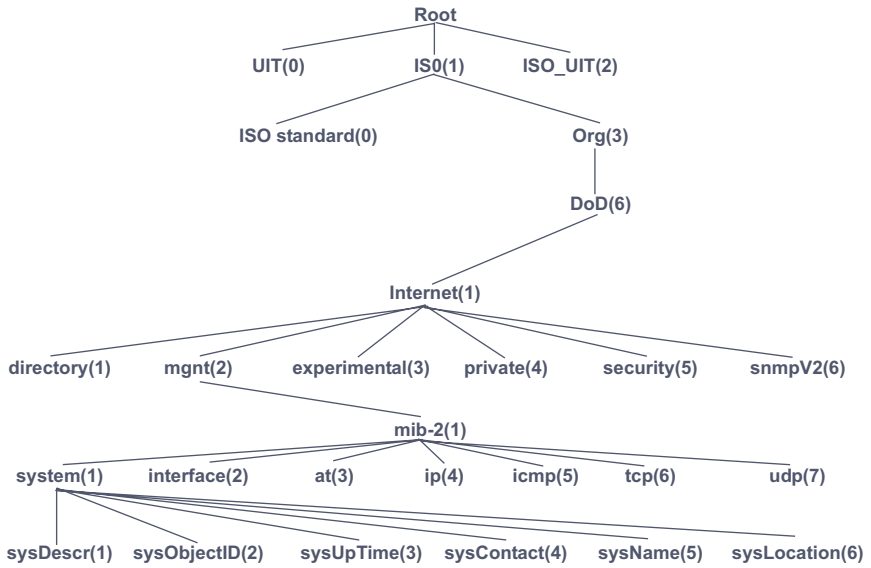


Figure 18.7 Arbre de nommage des objets SNMP.

La suite d'entiers qui désigne de manière non ambiguë un objet SNMP est **l'OID** de l'objet (*Object IDentifier*).

Les MIB privées

La MIB I contient 114 objets, la MIB II en définit 170. Malgré l'extension de la RMON MIB, les constructeurs ont constitué des MIB privées. Celles-ci sont développées dans la branche **private**. Par exemple, la MIB IBM contient quelque 600 objets. La figure 18.8 illustre l'utilisation de la branche *private*. L'accès aux variables des MIB privées est assuré par un agent spécifique qui effectue les conversions nécessaires : le **proxy-agent**.

Le proxy-agent permet ainsi le dialogue entre deux systèmes d'administration différents. Le principe du proxy-agent est illustré par la figure 18.9. Celui-ci peut être localisé dans le serveur pour l'utilisation d'une MIB privée, ou dans le manager si l'agent serveur n'est pas conforme au standard (conversion de protocole).

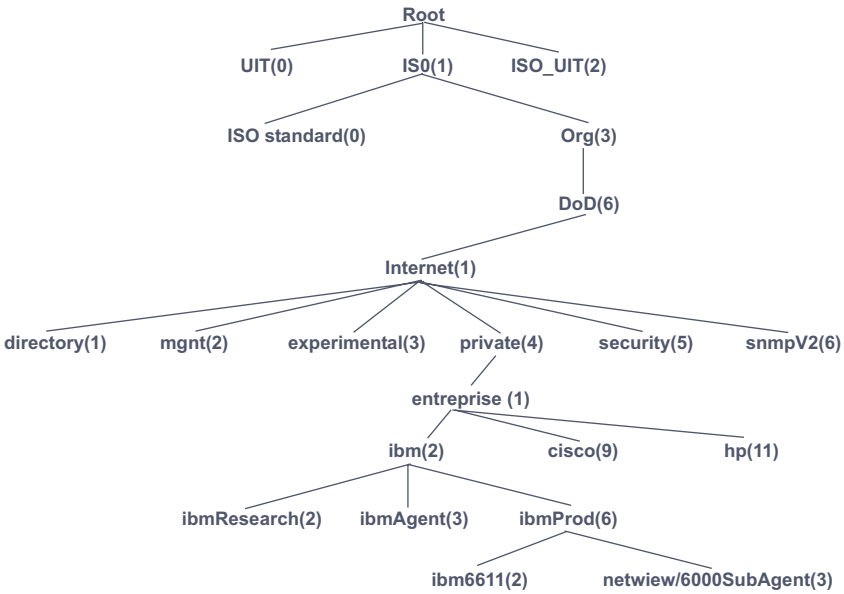


Figure 18.8 Extrait de la branche priate de la MIB IBM.

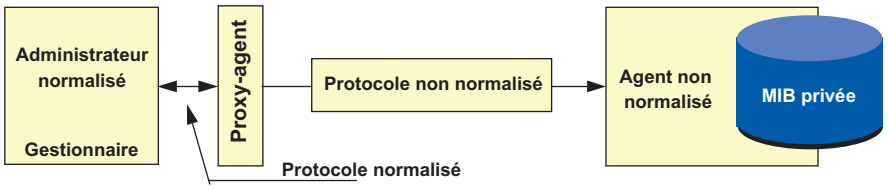


Figure 18.9 Principe d'un proxy-agent (mandataire).

Représentation codée des objets

Les requêtes SNMP identifient l'objet sollicité. Le codage de l'OID (*Objet Identifier*) suit les règles de codage des données définies par ASN1 : **BER** (*Basic Encoding Rules*) qui code le type, la longueur du champ et la valeur. Les deux premiers bits d'identification d'un objet permettent d'indiquer la nature de l'étiquette (00 universal, 01 application, 10 context, 11 private). Le troisième bit distingue un type primitif (0) d'un type construit (1). Les cinq suivants définissent la variable. SNMP n'utilise qu'un sous-ensemble de désignation des types (figure 18.10).

ID	Types Primitifs	Signification
2	INTEGER	Entier de taille arbitraire, utilisable pour définir des types énumérés
4	OCTET STRING	Liste d'octets (valeur 0 à 255)
5	NULL (NIL)	Objet sans type, peut être utilisé pour finir une liste
6	OBJECT IDENTIFIER	Identifie l'objet dans l'arbre de nommage
16	SEQUENCE	Autorise la construction de types complexes (similaire au record du Pascal)

Figure 18.10 Types « UNIVERSAL » d'ASN1 utilisés par SNMP

© Dunod – La photocopie non autorisée est un délit

Le codage des deux premiers entiers de l'OID suit des règles particulières. Compte tenu que le premier entier ne peut prendre que les valeurs 1 à 3 (UIT à Jonction UIT_ISO) et que le second est toujours inférieur à 40, les deux premiers entiers sont codés sur un seul octet : (A · 40 + B) où A représente le premier octet et B le second. Ainsi, l'objet **SysUpTime** (1.3.6.1.2.1.1.3), précédemment défini, est codé (figure 18.11) :

Type	Longueur	Valeurs
OBJECT IDENTIFIER	6	(1 · 40 + 3), 6, 1, 2, 1,1, 3
0x06	0x7	0x2B 0x06 0x01 0x02 0x01 0x01 0x03

Figure 18.11 Codification de l'objet *SysUpTime*.

18.3.3 Le protocole SNMP

Les protocoles SNMPv1 et v2 utilisent le même format de message (figure 18.12). Le champ *version number* vaut 0 (SNMPv1) ou 1 (SNMPv2). Le champ *community string* correspond à un mot de passe. Transmis en clair sur le réseau, il définit les droits d'un utilisateur sur une branche de la MIB (*MIB views*), ce n'est nullement un élément de sécurité.

Les primitives **GetRequest**, **GetResponse**, **GetNextRequest** et **SetRequest** utilisent la même structure de données.

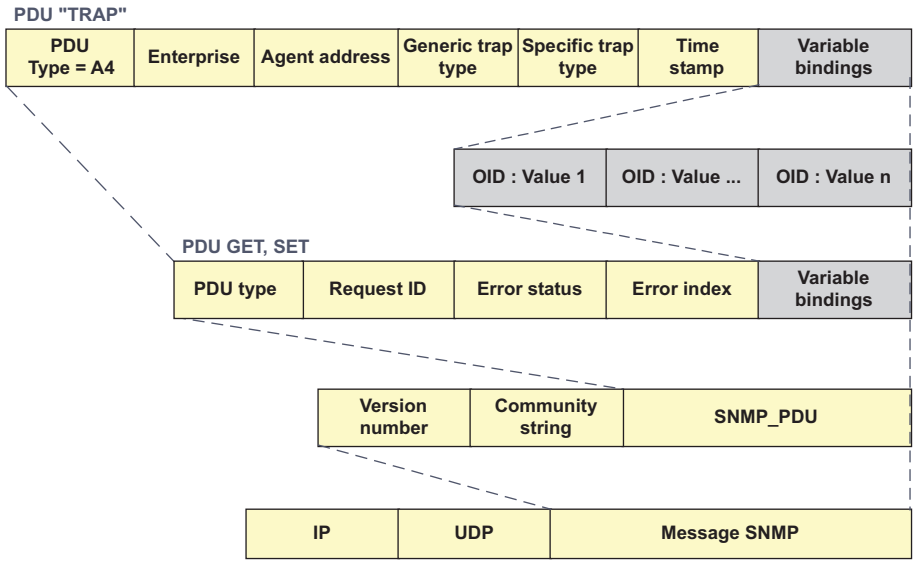


Figure 18.12 Format des messages SNMP.

Les primitives **Get**, **GetNextRequest**, **GetResponse** et **GetBulk** (SNMPv2) permettent, à l'initiative de la station d'administration, de lire les valeurs des objets de la MIB. La primitive **GetNextRequest** permet de récupérer les valeurs des objets qui suivent dans l'ordre lexicographique de l'arbre de nommage. Cette primitive permet de faire des appels récursifs. Cette primitive génère un trafic important, la version 2 a introduit la primitive **GetBulk** qui limite le nombre de variables retournées (*max-repetition*). La primitive **Set** permet de fixer une valeur à un objet. Ces primitives sont acquittées par la primitive **GetResponse**. Les primitives de type

Event (**Trap** et **Trap-SNMPv2**) sont émises, par l'agent à destination de la station d'administration, sur condition d'alerte, elles ne sont pas acquittées.

Les apports de SNMPv2 sont essentiellement :

– Un nouveau modèle administratif, l'entité SNMPv2 peut à la fois être *manager* et agent.
– L'introduction de la notion de dialogue de *manager* à *manager* (primitive *inform*).
– L'amélioration de la modélisation des objets, mais celle-ci reste proche de celle de la v1.
– La définition d'une nouvelle primitive (*GetBulk*).
– L'amélioration des messages de type *Trap* (*snmpv2*_trap).
– L'introduction de mécanismes de sécurité qui garantissent l'authentification par message digest (MD5), la confidentialité des messages SNMP par cryptographie (DES) et un mécanisme d'anti-rejeu par synchronisation des horloges. Enfin, le support multiprotocole (UDP, OSI...).

La version 3 transpose le modèle client/serveur de la v1 et v2 en un modèle *peer-to-peer*. La différentiation agent/*manager* est remplacée par celle plus générale d'entité SNMP (*snmp entity*). Malgré les apports des versions 2 et 3, notamment en matière de sécurité, la version 1 reste la plus utilisée.

18.4 SNMP ET ISO

Indépendamment de l'aspect orientation objet précédemment abordé, SNMP et ISO diffèrent essentiellement par la méthode de collecte des informations. SNMP travaille dans le mode sollicitation (*polling*) et ne peut interroger qu'un objet SNMP à la fois. Cette contrainte rend le protocole bavard. SNMP est peu adapté à la gestion de vastes réseaux. SNMP v2 pallie ce défaut en implémentant une nouvelle fonction : *Bulk Data Transfert*, qui autorise l'interrogation et la réponse de plusieurs objets. L'utilisation de proxy-agents permet de limiter le dialogue sur le WAN, le dialogue est SNMP entre le proxy-agent et l'organe administré, le proxy-agent ne transmettant au manager que les alertes.

Outre le faible nombre d'objets gérés, le reproche le plus courant fait à SNMP MIB1 est le manque de sécurité (une table de routage peut circuler en clair sur le réseau). Ces deux aspects sont corrigés par la MIBII, malheureusement peu implémentée.

Le protocole CMIS/CMIP d'ISO est plus adapté aux grands réseaux. Cependant il est très gourmand en ressources et les systèmes administrés n'implémentent que des agents SNMP. Dans ces conditions, un protocole intermédiaire, simplification du protocole CMIP, **CMOT** (*CMIP over TCP/IP*) a été défini pour utiliser les agents SNMP des réseaux TCP/IP dans les environnements de gestion OSI. À cet effet, une couche spécifique de présentation (**LPP**, *Lightweight Presentation Protocol*) a été définie au-dessus d'UDP, elle sert d'interface entre le monde TCP/IP et le monde OSI

18.5 LES PLATES-FORMES D'ADMINISTRATION

Les outils d'administration se répartissent en trois catégories :

– les systèmes de gestion des couches basses,

© Dunod – La photocopie non autorisée est un délit

– les hyperviseurs donnant une vue d'ensemble du réseau,
– les systèmes d'exploitation avec administration partiellement intégrée.

18.5.1 Les outils d'administration des couches basses

Dans cette catégorie, on trouve les consoles d'administration de câblage et les analyseurs de protocoles. Les gestionnaires de câblage permettent de suivre les évolutions du câblage et le brassage de celui-ci. Compte tenu de la charge de travail imposée par l'acquisition préalable des données et la mise à jour des évolutions, ces outils ne sont justifiés que pour les réseaux importants en nombre de prises.

Les sondes sont des éléments insérés dans un réseau pour en surveiller le fonctionnement. Elles fournissent, en temps réel, toutes les informations utiles au gestionnaire pour connaître l'état actuel de son réseau (taux d'erreurs, trafic...).

18.5.2 Les hyperviseurs

Les hyperviseurs sont de véritables plates-formes complètes d'administration de réseau. Ils permettent de superviser le réseau global de l'entreprise. Offrant les services d'une administration propriétaire (ex. : NetView d'IBM pour le réseau SNA) ou ouverte (ex : OpenView d'HP pour les environnements Unix), les hyperviseurs offrent une vue d'ensemble du réseau (état des liens, des nœuds, d'un port d'un routeur, d'une carte...).

18.5.3 Les systèmes intégrés au système d'exploitation

Les **NOS** (*Network Operating System*) comportent un ensemble d'outils non seulement pour la gestion des utilisateurs, des ressources et de la sécurité, mais aussi de supervision du fonctionnement général du réseau et tout particulièrement de la machine serveur (charge du CPU, *swapping*...).

18.6 CONCLUSION

Dans les réseaux de petites et moyennes importances, l'administration de réseau est souvent perçue comme une tâche superflue, chaque utilisateur pouvant être vu comme une « sonde ». L'ouverture des réseaux et leur nécessaire sécurisation ont fait prendre conscience des enjeux : le concept d'administration est aujourd'hui appréhendé dès la conception des réseaux. Cependant, bien que l'interface commune soit aujourd'hui du type navigateur web (**WBEM**, *Web-Based Enterprise Management*), les solutions propriétaires dominent le marché.

EXERCICES

Exercice 18.1 Analyse de trace SNMP

Un analyseur de protocole a relevé la trace suivante, il s'agit d'une trame Ethernet, contenant une requête SNMP.

```
Captured at:  +00:03.004
Length: 100    Status: Ok
OFFST DATA                                                    ASCII
0000: 00 A0 24 BD 75 DB 08 00 02 05 2D FE 08 00 45 00  ..$.u.....-...E.
0010: 00 52 3C EF 00 00 1C 06 A4 FF 80 00 64 00 D0 80  .`<.........d...
0020: 08 29 0A CF 00 A1 47 A8 BA 20 01 A3 96 14 50 18  .)...+G.. ....P.
0030: 20 00 72 D4 00 00 30 28 02 01 00 04 06 70 75 62   .r...0c.....pub
0040: 6C 69 63 A0 1B 02 04 03 05 52 AE 02 01 00 02 01  lic.............
0050: 00 30 0D 30 0B 06 07 2B 06 01 02 01 01 03 05 00  .0.0...+........
0060: 9F 59 6E FC                                      .Yn.
```

Les règles de codage des SNMP_PDU sont données ci-dessous.

```
Message SNMP DEFINITION ::=
BEGIN
 MESSAGE_SEQUENCE ::= SEQUENCE
            { version        Integer        -- Version = 0  pour  MIB 1
              commity        Octet String   -- "Mot de passe" de longueur variable
              data           Any            -- Données du message
            }
 PDUs :: = CHOISE
            { gest_request          GetRequest_PDU,
              gest_next_request     GetNextRequest_PDU,
              get_response          GetResponse_PDU,
              set_request           SetResponse_PDU,
              trap                  Trap_PDU
            }
END

GetRequest_PDU ::= [0] Implicit Sequence
            { request_ID        Request_ID,    -- Identification du couple question/réponse
              error_status      ErrorStatus,   -- Toujours à 0
              error_index       Error_Index,   -- Toujours à 0
             variable_bindlist  VarBindList    -- Liste OID et valeurs dans PDUs réponse
            }
```

Figure 18.13 Format général des messages SNMP et de la PDU GetRequest.

Décodez cette trame, et analysez les champs de la SNMP_PDU transportée.

© Dunod – La photocopie non autorisée est un délit

Exercice 18.2 SNMP et charge du réseau

La taille moyenne d'un message SNMP étant supposée de 100 octets, quelle est l'influence de la consultation de 100 objets SNMP à travers un lien WAN si la période de polling est fixée à 10 s et que le débit du lien est de 64 kbit/s.

Chapitre **19**

Introduction à l'ingénierie des réseaux

19.1 GÉNÉRALITÉS

Pour satisfaire les besoins de télécommunication des entreprises, les opérateurs (prestataires de service de télécommunication) offrent deux types de service, les services supports et les téléservices.

Les **services supports** consistent à fournir à un abonné (l'entreprise) un lien de communication (support physique ou virtuel) entre deux points (ligne point à point) ou entre un et plusieurs points (ligne multipoint). Les services offerts peuvent être simples comme la location d'un lien (liaison louée). L'opérateur met alors à disposition de l'entreprise un lien et les organes d'extrémités d'accès (modems). Lorsque ce support est numérique l'opérateur ne s'engage que sur le débit nominal du lien et le taux d'erreur. Quand il s'agit d'un lien analogique seuls la bande passante et le rapport signal à bruit sont garantis. Les liaisons louées sont utilisées pour réaliser des liaisons point à point et les réseaux privés d'entreprise.

Une alternative à la réalisation d'un réseau privé consiste à relier les divers établissements d'une entreprise via un réseau de transport public. L'opérateur assure alors le raccordement des sites de l'abonné à son réseau. Les caractéristiques du raccordement dépendent alors du réseau de l'opérateur (débit, protocole...).

Les **téléservices** constituent une offre plus élaborée. L'opérateur fournit alors un moyen complet de communication. Dans cette catégorie, on trouve la téléphonie analogique (RTC) et numérique (RNIS), les services de messagerie, les services télématiques (vidéotex)...

Le type de service requis est déterminé en fonction des services attendus (téléservices) ou de critères techniques (services supports). La politique tarifaire de l'opérateur, l'évolution prévisible des besoins et la reprise de l'existant sont les éléments déterminants devant guider le choix.

L'ingénierie des réseaux recouvre l'ensemble des moyens mis en œuvre pour le choix d'une solution de télécommunication et la réalisation d'un réseau de télécommunication (topologie, dimensionnement, évaluation des performances, optimisation...).

19.2 SERVICES ET TARIFICATION

D'une manière générale, toute fourniture de service comprend : des frais d'accès au service (frais d'établissement ou de mise en service), un abonnement et une redevance d'usage. Les frais d'établissement sont comptés pour chaque raccordement au service. Ainsi, lors de l'installation d'une liaison louée, la redevance est due pour chaque extrémité du lien. La redevance d'usage dépend de certains critères dont :

– le temps et la distance (réseau téléphonique), ces éléments pouvant subir des modulations tarifaires en fonction des créneaux horaires d'utilisation ;
– le volume de données transféré (réseau X.25).

La redevance peut aussi être forfaitaire et déterminée en fonction des caractéristiques du raccordement. Ainsi pour les liaisons louées, la redevance d'usage est fixée en fonction de la distance séparant les sites raccordés et du débit nominal de la ligne. Quant à la redevance d'usage des réseaux de données, elle dépend du débit nominal du lien et des descripteurs de trafic définis à l'abonnement (débit moyen garanti, débit de crête permis, nombre de liaisons virtuelles utilisées...). L'opérateur fournit généralement les moyens d'accès. Dans ce cas, leur location est comprise dans la redevance mensuelle.

Le choix entre la réalisation d'un réseau privé, à base de liens privés ou publics, ou le recours aux services d'un opérateur est essentiellement motivé par des économies d'échelle, la maîtrise des coûts et des techniques (protocole, voix/données...) ou certaines spécificités de l'entreprise comme la sécurité des informations (confidentialité...).

19.3 ELÉMENTS D'ARCHITECTURE DES RÉSEAUX

19.3.1 Structure de base des réseaux

En principe, un réseau comporte deux sous-ensembles : le **réseau dorsal** ou réseau de transit (backbone) et le **réseau de desserte** ou réseau capillaire ou encore réseau de bas niveau (figure 19.1). Le premier est un réseau de concentration qui assure la mise en relation (connectivité) des différentes composantes du réseau de desserte. Le second assure la distribution du service aux abonnés, il est composé d'un ensemble de liens et de concentrateurs. Un niveau de concentration élevé optimise le réseau mais le fragilise.

Le choix de la localisation et du nombre de points d'accès détermine le coût de raccordement des abonnés (sites terminaux de l'entreprise ou abonnés d'un opérateur). De ce fait, il existe une relation étroite entre le graphe du réseau dorsal et le graphe du réseau de desserte.

La réalisation d'un réseau privé dans le contexte d'une entreprise donnée est relativement simple, l'emplacement des points d'accès au réseau est parfaitement déterminé. Dans ces réseaux, ce sont les points de concentration et le mode de liaison entre les différents sites qu'il convient d'optimiser. La topologie est généralement arborescente, le maillage n'intervient qu'en second lieu et essentiellement pour des critères de sécurité (redondance de liens).

Celle des réseaux publics est plus complexe, non seulement les points d'accès sont nombreux, mais les points de concentration ne sont pas prédéterminés et les contraintes de qualité de service sont plus strictes. La solution optimale est généralement le résultat d'un compromis

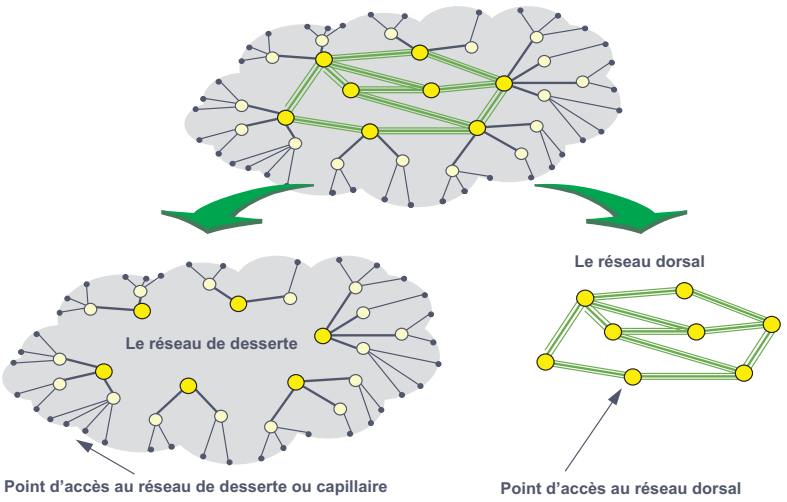


Figure 19.1 Architecture générale d'un réseau.

obtenu par itérations successives en formulant différentes hypothèses de positionnement des nœuds d'accès et de concentration.

Quelles que soient les hypothèses formulées, un réseau résultera de compromis entre performance, fiabilité et coût. En effet, un niveau de performance élevé nécessite un maillage élevé du réseau dorsal et un faible niveau de concentration dans le réseau de desserte, ce qui en accroît la fiabilité mais en augmente aussi le coût.

Il existe de nombreuses méthodes pour optimiser la topologie des réseaux selon un critère prédéterminé (coût, débit, performance...). Certaines essaient de trouver la solution optimale, elles sont difficiles à mettre en œuvre et résistent mal à l'introduction de nouvelles contraintes ou à une évolution des besoins. D'autres méthodes, dites heuristiques, ne cherchent pas à déterminer la solution optimale mais à s'en rapprocher le plus possible. Elles prennent facilement en compte de nombreuses contraintes. Leur principe est simple, à partir d'hypothèses sur le positionnement des composants, elles les réunissent deux à deux par le lien de moindre coût.

19.3.2 Conception du réseau de desserte

Du fait de la densité des points de concentration et des liaisons, le réseau de desserte est généralement le plus coûteux à réaliser. Aussi, c'est à partir de lui que la localisation des points d'accès au réseau dorsal est déterminée. Ainsi, le réseau de desserte est étudié nœud par nœud en formulant diverses hypothèses sur la localisation des nœuds du niveau supérieur. Après avoir défini les niveaux de concentration, on affecte les concentrateurs de niveau N aux concentrateurs de niveaux N – 1, en respectant les contraintes de nombre de branches (fiabilité), de débit, de coût...

Les deux méthodes exposées ci-dessous dérivent de l'algorithme de Prim et de Krustal. L'algorithme de Prim sous contrainte consiste à :

– formuler une hypothèse sur le positionnement du nœud de concentration principal (accès au réseau dorsal...),
– définir les points à raccorder,

© Dunod – La photocopie non autorisée est un délit

– déterminer le coût (C_{xy}) de toutes les liaisons une à une (matrice des coûts) entre les différents nœuds du réseau,
– trier les liens par ordre croissant des coûts,
– considérer le nœud de concentration comme nœud central et l'inclure en premier dans l'arbre,
– tant que les contraintes fixées pour les raccordements sont respectées (débit maximal à concentrer, nombre de liens regroupés...) relier le point dont le coût de connexion est le plus faible à l'un des points déjà contenus dans l'arbre,
– réitérer l'action précédente jusqu'à ce que tous les nœuds soient reliés, en ne retenant que les liaisons ne faisant pas de boucle et qui respectent les contraintes imposées.

La mise en œuvre de l'algorithme de Kruskal sous contrainte est aussi simple, elle comprend les étapes suivantes, les 4 premières étapes étant identiques à celles de l'algorithme de Prim :

– construire la première branche en réunissant les 2 nœuds dont le coût de la liaison est le plus faible ;
– réitérer l'action précédente jusqu'à ce que tous les nœuds soient reliés, en ne retenant que les liaisons ne faisant pas de boucle et qui respectent les contraintes imposées (débit global, nombre de liens sur un même point de concentration...) ;
– quand pour une branche, un regroupement ne peut plus être opéré (contrainte atteinte), le regroupement est considéré comme un sous-arbre qui sera relié au nœud de concentration supérieur élu, par son nœud le plus proche.

	a	b	c	d	e	f	g	h	i	j	k
a		35	40	74	69	42	40	64	60	25	43
b			31	61	80	75	55	95	91	60	76
c				35	50	84	32	88	95	84	82
d					49	89	51	111	124	96	116
e						58	29	74	96	77	97
f							38	23	37	29	41
g								60	74	50	70
h									25	41	44
i										35	27
j											20

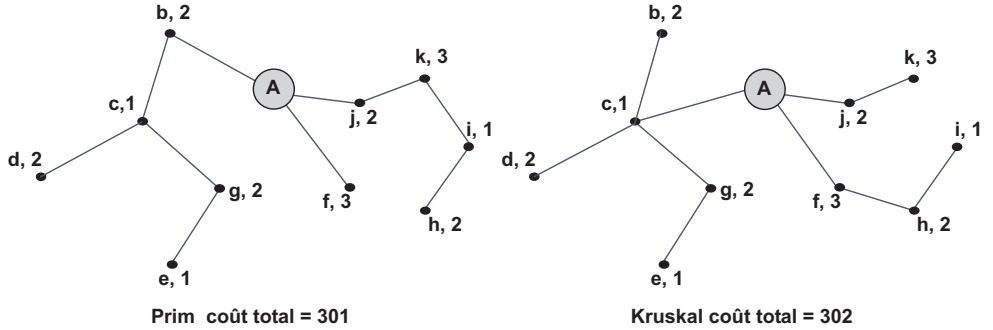


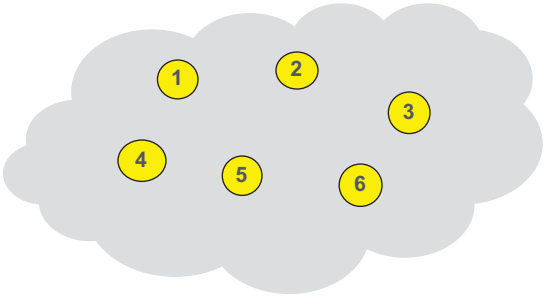
Figure 19.2 Matrice des coûts et arbres à coût minimal de Prim et Kruskal.

La figure 19.2 illustre ces deux méthodes. Le coût retenu est la distance séparant les différents nœuds. Le nœud « ***A*** » pouvant représenter le nœud de concentration de niveau supérieur ou le site informatique principal d'une entreprise vers lequel tous les sites doivent converger. La contrainte retenue ici a été le débit, celui-ci ne devant pas excéder pour cet exemple 8. Le débit requis par chaque nœud figure à droite de son identification. Bien que les graphes résultants diffèrent, les coûts sont ici très proches.

19.3.3 Conception du réseau dorsal

La recherche de performance et de fiabilité conduit à multiplier les liens internœuds (maillage) de façon à assurer une redondance de route (fiabilité) et à minimiser le nombre de sauts (performance). Plusieurs méthodes existent, l'une des plus simples, la méthode de Steiglitz, donne des résultats satisfaisants pour la plupart des réseaux d'entreprise. Cette méthode, illustrée figure 19.3, consiste à :

- définir le positionnement de tous les nœuds et leur connectivité (nombre de liens aboutissant à un nœud),
- attribuer, arbitrairement, un poids à chaque nœud,
- relier le nœud de plus faible connectivité (en cas d'égalité prendre le nœud de plus faible poids) à son voisin de moindre coût,
- répéter l'opération tant que la connectivité de chaque nœud n'est pas atteinte,
- modifier les poids attribués, refaire le graphe jusqu'à trouver celui de coût minimal.



Points d'accès au réseau dorsal

	1	2	3	4	5	6
1		52	101	40	52	95
2	52		50	85	57	55
3	101	50		123	80	32
4	40	85	123		48	107
5	52	57	80	48		60
6	95	55	32	107	60	

Matrice des coûts

Figure 19.3 Conception du réseau dorsal.

Au début, tous les nœuds ayant la même connectivité (0), on prend le nœud de poids le plus faible soit 1, le nœud 4 est le voisin à coût minimal, on relie 1 à 4. Ensuite, on prend le suivant 2 (poids le plus faible) on le relie à 3 (coût le plus faible)... En final on obtient le réseau de la figure 19.4 (gauche). La partie droite de la figure représente le même réseau obtenu en changeant la valeur des divers poids.

En principe, la réalisation d'un réseau d'entreprise est plus simple : les points de concentration coïncident avec les points de consommation et sont déterminés (établissements de l'entreprise), beaucoup d'entreprises mettent en œuvre une topologie étoile autour de leur centre

© Dunod – La photocopie non autorisée est un délit

informatique principal. Lorsque les contraintes sont faibles en terme de débit, mais fortes en terme de coût, l'algorithme de Kruskal vu précédemment donne d'excellents résultats.

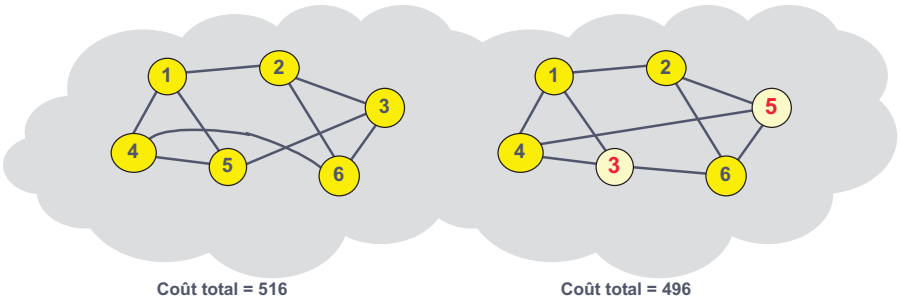


Figure 19.4 Graphe du réseau dorsal.

19.4 DIMENSIONNEMENT ET ÉVALUATION DES PERFORMANCES

19.4.1 Généralités

Evaluer les performances d'un réseau est une tâche essentielle, tant lors de la conception que durant tout le cycle de vie du système. Indépendamment de mesures concrètes (débit, temps de transit...), on utilise généralement un modèle mathématique du réseau (modélisation) permettant de déterminer le comportement du réseau en fonction de certains paramètres et de leur variation (trafic, état d'un lien...). Les éléments pris en compte diffèrent selon que le réseau est en mode circuits ou en mode paquets (figure 19.5) :

– Dans les réseaux en mode circuits (circuits physiques ou IT, Intervalle de Temps), la bande passante est affectée en permanence à un utilisateur, le mode de transfert est dit synchrone (bande passante fixée par le réseau). La problématique consiste à définir le nombre de liens (IT) en fonction du nombre de sessions utilisateurs par unité de temps (taux d'arrivée) et de la durée moyenne d'une session.

– Dans les réseaux en mode paquets, il n'y a pas de ressource affectée, la bande passante est partagée. Il n'y a pas de relation directe entre le débit de la source et celui du réseau, le mode de transfert est dit asynchrone. Soumis à des trafics sporadiques, et souvent sous-dimensionnés par rapport au trafic total à écouler, ils sont sensibles à la congestion. Les réseaux en mode connecté avec réservation de ressource relèvent à la fois du modèle des réseaux en mode circuit pour le nombre de connexions admises et du modèle des réseaux en mode paquet en ce qui concerne les performances.

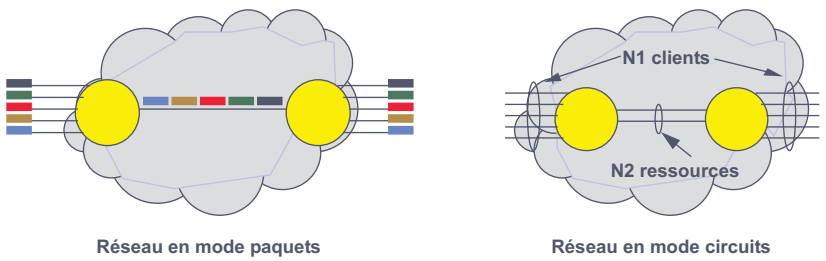


Figure 19.5 Les deux types de réseaux.

19.4.2 Les réseaux en mode circuit

Notion d'intensité de trafic

Lorsqu'un système établit une connexion permanente, le nombre de liens à établir est simple à définir. Si N sites doivent être reliés simultanément à un autre site, généralement désigné par site central, il est nécessaire de disposer de N lignes. Mais lorsque les systèmes d'extrémité n'établissent qu'une connexion temporaire, ce serait un gâchis de ressource que d'équiper le site central d'autant de lignes qu'il y a de possibilité de mise en relation. C'est notamment le cas pour un serveur de messagerie auquel se connectent une fois par jour les itinérants des sociétés pour y relever leur courrier, transférer leurs commandes et éventuellement télécharger les nouveaux tarifs.

Partant du principe que les sources sont indépendantes les unes des autres (les arrivées sont supposées suivre une loi de Poisson), il n'est pas improbable que, dans certaines circonstances, les arrivées dépassent les capacités de traitement du système. Dans ces conditions, les requêtes en surnombre sont soit éliminées soit mises en attente de libération d'un organe de traitement (support, ou autre). Sur ce principe, Erlang (mathématicien danois) a développé deux modèles l'un dit à refus ou blocage (**modèle B**), l'autre dit à attente (**modèle C**).

Les modèles ont été élaborés à partir de l'expression de la quantité de trafic à satisfaire dénommé **intensité de trafic** et exprimée en erlang par la relation :

$$E = \frac{1}{T}\int_0^T n(t)dt$$

ou plus simplement $E = NT/3\,600$

T est exprimé en secondes N : nombre de sessions par heure

E : charge de trafic en erlang[1].

Ainsi, 1 erlang représente l'occupation permanente d'un organe pendant 1 heure, ou l'occupation effective de 2 organes à 50 % (1/2 heure chacun) pendant la même période. L'intensité de trafic sur une ligne représente le taux de connexion de celle-ci, c'est-à-dire le temps d'appropriation de l'organe par unité de temps.

Modèle d'Erlang à refus (modèle B)

➤ Formule d'Erlang

Dans un système dit à pénurie de ressource, c'est-à-dire que le nombre de clients (n) est supérieur au nombre d'organes de traitement (m), Erlang a établi que la probabilité p de refus d'appel (facteur de blocage) par suite d'encombrement ou autre pour un trafic à écouler de E erlang est donnée par la relation (figure 19.6) :

$$p = \frac{E^m / m!}{\sum_{k=0}^{k=m} E^k / k!}$$

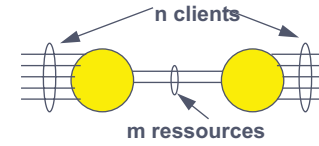


Figure 19.6 Formule d'Erlang à refus.

1. L'intensité de trafic est un nombre sans dimension.

© Dunod – La photocopie non autorisée est un délit

Cette formule a permis d'établir un abaque de dimensionnement appelé abaque d'Erlang représenté figure 19.7.

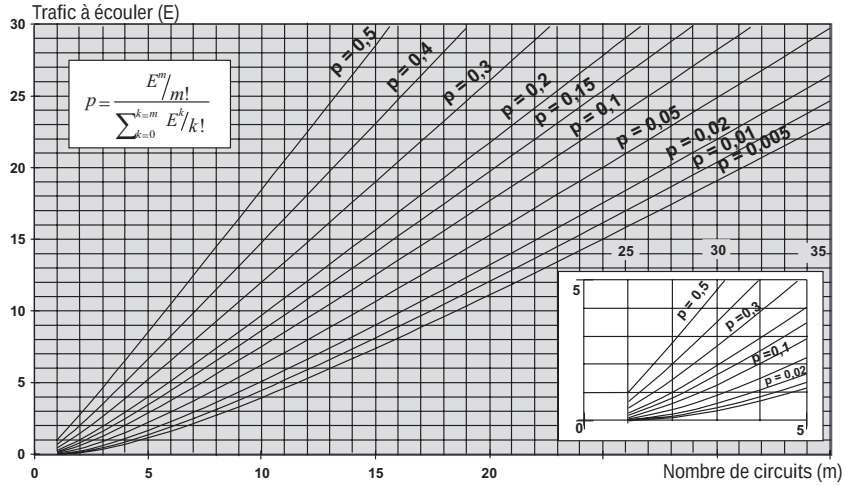


Figure 19.7 Abaque d'Erlang (refus).

➤ Trafic demandé, trafic écoulé, trafic perdu

Par suite des collisions d'appel (organes occupés), une partie du trafic à écouler ou trafic demandé est perdue. Le trafic perdu et celui demandé sont liés par la relation :

$$Trafic\ perdu = Trafic\ demandé \times p$$

où p est la probabilité de refus d'appel.

Le trafic réellement écoulé est alors :

$$Trafic\ écoulé = Trafic\ demandé - Trafic\ perdu = Trafic\ demandé(1 - p)$$

La figure 19.8 fournit quelques exemples pour un trafic de 0,9 erlang lorsque la ressource passe de 1 à 5 organes.

Trafic demandé	Ressources m	Probabilité de perte	Trafic perdu	Trafic écoulé
0,9 E	1	0,47	0,43	0,47
0,9 E	2	0,17	0,16	0,74
0,9 E	3	0,05	0,05	0,85
0,9 E	4	0,01	0,01	0,89
0,9 E	5	0,002	0,00	0,90

Figure 19.8 Trafic demandé, perdu et écoulé.

Modèle d'Erlang à attente (Modèle C)

Le modèle à attente suppose que toute demande ne pouvant être satisfaite est mise dans une file d'attente de capacité infinie et sera traitée dès qu'un organe se libère. C'est le cas notamment des processus dans les systèmes relais[2] (routeur...). Cependant, on peut admettre que ce modèle

2. On admettra que les mémoires sont, vis-à-vis du trafic, suffisamment dimensionnées pour être assimilable à une mémoire de capacité infinie.

s'applique aussi aux appels entrants des centraux téléphoniques d'entreprise. En effet, dans ces centraux, en cas d'occupation de l'appelé, l'appel entrant n'est généralement pas refusé mais mis en attente. Ce procédé monopolise une ressource en arrivée et n'écoule aucun trafic. Dans le modèle d'Erlang C, la probabilité p_a de mise en attente est donnée par la relation :

$$p_a = \frac{\left(E^m/m!\right) \cdot \left(\dfrac{m}{m-E}\right)}{\left[\displaystyle\sum_{k=0}^{k=m-1} E^k/k!\right] + \left[\left(E^m/m!\right) \cdot \left(\dfrac{m}{m-E}\right)\right]}$$

19.4.3 Les réseaux en mode paquets

Principe de la modélisation des réseaux

L'échange d'information entre deux applications ou entre une application et un terminal est généralement variable en terme de volume à échanger et de fréquence des échanges. Si l'on prend en compte l'écart de débit, entre les systèmes locaux et les liens d'interconnexion, l'organe d'interconnexion du système de transmission (routeur, FRAD[3], modem...) constitue un goulet d'étranglement. Il en résulte que les messages ne seront pas transmis instantanément, ils seront placés dans une file d'attente (queue) avant d'être traités par le système de transmission. En première approximation, on peut modéliser un système de transmission comme étant constitué d'une simple ligne reliant les deux systèmes d'extrémité (figure 19.9).

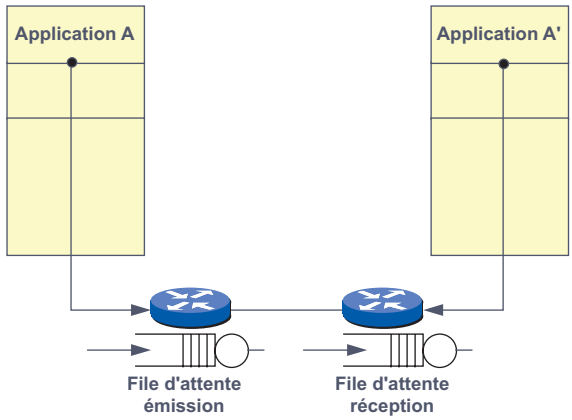


Figure 19.9 Modélisation simplifiée d'un système de transmission.

Le temps de réponse du système pour un message peut s'exprimer par la relation :

$$T_r = T_p + T_t + T_q$$

où T_r est le temps de réponse du système, T_p le temps de propagation sur le support, T_t le temps de traitement par les systèmes d'interconnexion, T_q le temps de séjour dans les systèmes ou temps de queue.

3. FRAD, *Frame Relay Access Device*.

© Dunod – La photocopie non autorisée est un délit

Lorsque le nombre de messages à traiter augmente, T_q devient prépondérant par rapport aux autres éléments, ces derniers pourront alors être négligés. Le problème consiste donc à calculer le temps de queue en fonction des caractéristiques du système (nombre d'items traités par unité de temps ou μ), de la longueur du message (L) et du débit de la ligne du système (D). Il est possible aussi, à partir de ces éléments, de déterminer les caractéristiques du système pour répondre aux contraintes temporelles des applications.

Notions de files d'attente

➤ Relation de base, formule de Little

Dans un système à file d'attente en équilibre (figure 19.20), c'est-à-dire que le nombre moyen d'entrées (λ) est égal au nombre moyen de sorties par unité de temps, le nombre moyen d'items (clients) dans le système N est donné par la relation :

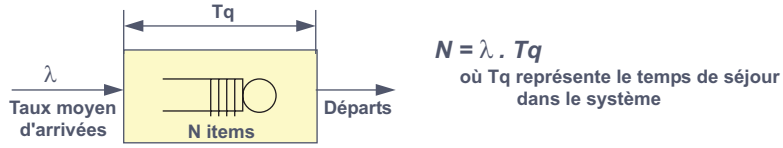


Figure 19.10 Formule de Little.

Si la condition d'équilibre est respectée, la relation de Little s'applique à tous les types de files d'attente.

➤ Les files d'attente M/M/1/∞

Le modèle M/M/1/∞ est le modèle plus simple retenu pour la modélisation des réseaux. Selon la notation de **Kendal** cette file est caractérisée par :

- **M**, processus Markovien en entrée (distribution exponentielle des arrivées),
- **M**, processus Markovien en sortie,
- **1**, il n'y a qu'un seul processeur (système mono-serveur),
- ∞, la file d'attente a une capacité infinie, aucun item entrant n'est perdu.

Dans ce type de processus, on considère les arrivées indépendantes les unes des autres, ce qui est généralement le cas des processus informatiques où les systèmes d'extrémité s'échangent des messages indépendamment les uns des autres.

Dans le système M/M/1/∞ (figure 19.11), on désigne par λ le taux d'arrivée des items dans la file, par *ta* le temps de séjour dans la file d'attente, par *ts* le temps de traitement par le système (son inverse 1/ts représente le nombre d'items traités par unité de temps ou taux de service et est désigné par μ) et *tq* le temps qui s'écoule entre l'entrée d'un item dans le système et sa sortie (temps de séjour). Le nombre d'items en attente de traitement *Na* et le nombre d'items en cours de traitement *Ns* sont une fonction directe du temps d'attente ou de traitement et du taux d'arrivée :

$$Na = \lambda ta \quad \text{et} \quad Ns = \lambda ts$$

Le nombre d'items N dans le système peut s'écrire (décomposition de la formule de Little) :

$$N = Na + Ns = \lambda(ta + ts) \quad \text{(relation 1)}$$

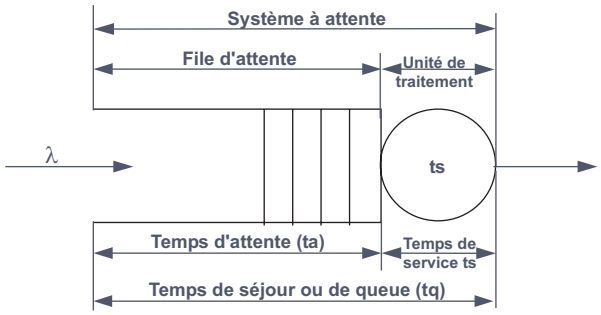


Figure 19.11 Modélisation d'une file M/M/1/∞.

Pour tout nouvel entrant dans le système, le temps d'attente correspond au temps nécessaire pour traiter tous les items déjà présents dans la file soit :

$$ta = N \cdot ts \quad \text{(relation 2)}$$

Dans la relation 1, en remplaçant la valeur de *ta* par celle obtenue dans la relation 2 :

$$N = \lambda(ta + ts) = \lambda(\text{Isys} \cdot ts + ts) = N \cdot \lambda ts + \lambda ts$$
$$N - N \cdot \lambda ts = \lambda ts$$
$$N(1 - \lambda ts) = \lambda ts$$
$$N = \lambda ts/(1 - \lambda ts)$$

Si on pose μ = *1/ts* (taux de service du système), la charge du système ρ est représentée par la relation :

$$\rho = \lambda/\mu = \lambda ts$$

on obtient :

$$N = \frac{\rho}{1 - \rho}$$

En reportant cette valeur dans la relation 2, on obtient :

$$ta = \frac{\rho}{1 - \rho} ts$$

Le temps de séjour dans le système ou temps de queue est alors :

$$tq = ta + ts = ts\left(1 + \frac{\rho}{1 - \rho}\right) = ts\left(\frac{1}{1 - \rho}\right)$$

Étudions la variation du temps de séjour dans la file d'attente quand la charge du système varie de 10 à 100 % par pas de 10 %.

Le temps de séjour dans la file est relativement faible jusqu'à une charge de 50 %. Au-dessus de cette charge, le temps de séjour croît très vite (figure 19.12). Compte tenu qu'un système est généralement étudié pour un trafic moyen, pour garantir, lors de trafic de crête, des performances acceptables, il convient de le dimensionner pour que la charge moyenne de celui-ci n'excède pas 50 %.

© Dunod – La photocopie non autorisée est un délit

Charge	10 %	20 %	30 %	40 %	50 %	60 %	70 %	80 %	90 %	100 %
$\rho/(1-\rho)$	0,1/0,9	0,2/0,8	0,3/0,7	0,4/0,6	0,5/0,5	0,6/0,4	0,7/0,3	0,8/0,2	0,9/0,1	1/0
ta=ts . $\rho/(1-\rho)$	0,11	0,25	0,42	0,66	1	1,5	2,3	4	9	∞
	Temps d'attente acceptable					Temps d'attente prohibitif				

Figure 19.12 Évolution du temps de séjour en fonction de la charge.

➤ Application au calcul du débit d'une ligne

En exprimant la charge d'une ligne en fonction des caractéristiques du message (L, longueur en bits) et du système (D, débit de la ligne en bit/s), on obtient :

$$\rho = \frac{\lambda}{\mu} = \frac{\lambda}{\frac{1}{ts}} = \lambda ts = \frac{\lambda L}{D}$$

Le temps séjour dans le système ou temps de queue est alors :

$$tq = ts\left(\frac{1}{1-\rho}\right) = \frac{L}{D}\left(\frac{1}{1-\frac{\lambda L}{D}}\right) = \frac{L}{D-\lambda L}$$

avec $D > \lambda L$

Mais, compte tenu que nous venons d'établir qu'un système ne doit pas être chargé à plus de 50 %, le débit minimal requis (D_{min}) pour la ligne est de :

$$D_{min} \geqslant 2\lambda L$$

➤ File d'attente en série

Lorsque deux files d'attente sont en série, si la file d'attente d'entrée est du type M/M/1/∞, les arrivées suivent une loi de Poisson ainsi que les sorties. Dans ces conditions, les entrées de la suivante respectent une loi de Poisson ; cette file est donc aussi poissonienne et de type M/M/1/∞. Le temps de traversée global est la somme des temps de traversée de chacune des files (figure 19.13).

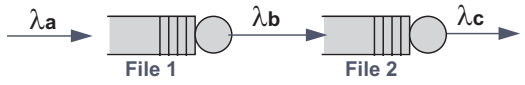


Figure 19.13 Réseau ouvert de files d'attente en série.

Un réseau peut être modélisé comme une succession de files d'attente, et chaque élément actif du réseau (routeur, commutateur, FRAD...) peut lui-même être considéré comme deux files d'attente en série (figure 19.14).

➤ File d'attente à entrées multiples

On montre, que si les messages ont la même longueur moyenne sur toutes les voies incidentes, la file d'attente est équivalente à une file d'attente à une seule entrée où le taux d'arrivée est la somme des taux d'arrivée : $\lambda = \Sigma\ \lambda_i$ (principe de la superposition, figure 19.15).

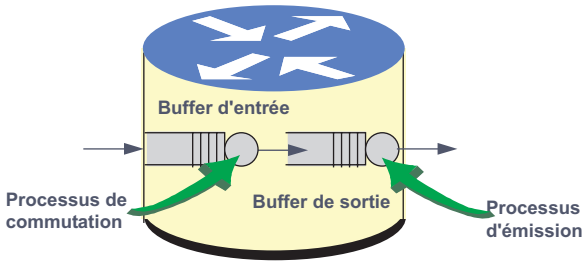


Figure 19.14 Modélisation simplifiée d'un élément actif.

Par exemple, une file d'attente à entrées multiples peut correspondre à un nœud intermédiaire sur lequel convergent plusieurs liens

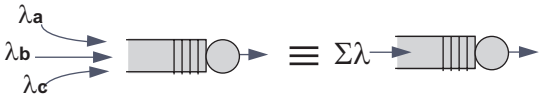


Figure 19.15 File d'attente avec entrées multiples.

➤ Les files d'attente M/M/1/K

Le modèle M/M/1/∞ considère la file d'attente comme infinie, c'est-à-dire que tout item entrant sera traité, cette hypothèse simplificatrice est satisfaisante dans la majorité des cas. Mais lorsque le réseau est chargé, les files d'attente physiques (tampon ou buffer) n'étant pas de taille illimitée, la probabilité pour qu'un item entrant ne puisse être accepté n'est pas nulle (figure 19.16).

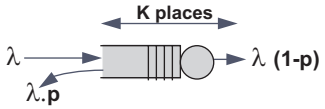


Figure 19.16 File d'attente à capacité limitée.

Si K est la taille de la file d'attente et que celle-ci contient déjà n items, la probabilité pour qu'un nouvel arrivant soit perdu (p_n) est :

$$\text{si} \quad \rho \neq 1 \qquad p_n = \frac{\rho^n(1-\rho)}{1-\rho^{K+1}} \quad \text{avec} \quad 0 \leqslant n \leqslant K$$

$$\text{si} \quad \rho = 1 \qquad p_n = \frac{1}{K+1} \quad \text{avec} \quad 0 \leqslant n \leqslant K$$

Application à la modélisation d'un réseau

Soit le réseau représenté par la figure 19.17, si on admet que tout item entrant est sortant (système en équilibre), il peut être modélisé simplement en remplaçant chaque élément actif par une file d'attente. Il est alors possible à partir d'un trafic d'entrée (E) de déterminer le comportement du réseau pour les données en transit de E vers S.

© Dunod – La photocopie non autorisée est un délit

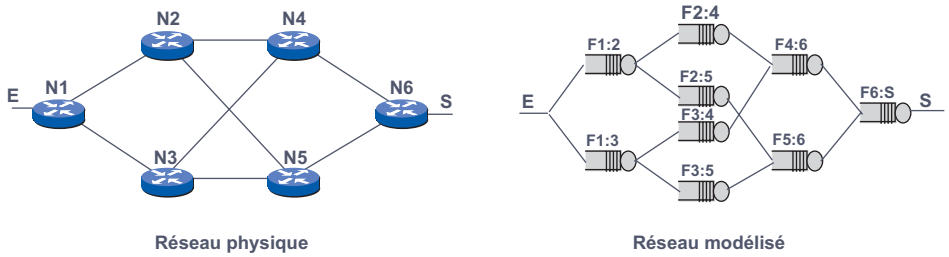


Figure 19.17 Modélisation d'un réseau.

Pour définir le comportement global du réseau, il faut quantifier le trafic entre tous ses points d'entrée et de sortie (matrice de trafic). En superposant chacun des trafics élémentaires dans chaque file, on en détermine le comportement point à point puis on en déduit le comportement global du système.

19.5 CONCLUSION

Ce chapitre a pour objectif d'initier aux méthodes utilisées pour la réalisation, le dimensionnement et les mesures de performances des réseaux. Ces techniques conduisent à construire des modèles mathématiques de plus en plus élaborés dont l'étude sort du cadre de cet ouvrage. Devant la complexité des réseaux et les exigences des utilisateurs, les modèles deviennent de plus en plus complexes et la recherche de nouvelles techniques de modélisation permanente.

EXERCICES

Exercice 19.1 Service de vidéotex

Une entreprise de vente par correspondance outre les accès Internet continue d'offrir à ses clients un service de prise de commande et de consultation de l'état de celles-ci sur Minitel. Compte tenu de la baisse d'activité de ce service, l'entreprise doit redimensionner ce service. Les données en prendre en compte sont : une transaction de commande dure en moyenne 2 minutes et on admet qu'à l'heure de pointe il y a 600 demandes de connexion. Pour satisfaire pleinement sa clientèle, l'entreprise désire que le taux de refus, suite d'un manque de ressource, ne soit pas supérieur à 1 %. Le service vidéotex est disponible sur un réseau X.25 et accessible via le réseau téléphonique commuté. On vous demande :

– Combien de circuits virtuels l'entreprise doit-elle souscrire à l'opérateur X.25 ?

– Dans les conditions établies précédemment, combien de demandes de connexion pourront être formulées en 1 heure, si on admet un taux de refus de 2 % ?

Exercice 19.2 Informatisation d'un magasin

Une chaîne de distribution d'électroménager désire construire une nouvelle surface de vente. Le nouveau magasin sera équipé de terminaux passifs reliés au système informatique central de l'entreprise. Les applications informatiques sont de quatre natures :

– accueil clientèle et vente : des terminaux (terminal point de vente) permettent aux vendeurs de renseigner les clients sur la disponibilité d'un produit, le poste est alors immobilisé une minute environ. Lorsque le client acquiert l'objet (6 fois sur 10 en moyenne), la prise de commande et la mise à jour des stocks monopolisent le poste environ 3 minutes supplémentaires ;

– le poste d'enlèvement des achats sera doté de terminaux pour la consultation de la localisation des objets retirés : l'immobilisation du poste est estimée à une minute par enlèvement (chaque vente donne lieu à enlèvement) ;

– l'encaissement : on estime qu'il ne doit y avoir jamais plus de cinq clients en attente devant un poste d'encaissement et qu'un client s'impatiente si son temps d'attente, avant traitement, dépasse 10 minutes ; l'opération d'encaissement dure en moyenne 3 minutes ;

– le système comportera en plus les postes comptables au nombre de 2 (1 par agent). Chaque comptable effectue au plus 20 transactions/jour régulièrement réparties dans la journée et travaille 8 heures/jour.

On estime qu'à l'heure de pointe, le jour le plus chargé, 100 clients en moyenne seront renseignés par les vendeurs. On demande :

– le nombre de terminaux de caisse ;

– le nombre de terminaux au poste enlèvement, si on admet que dans 80 % des cas, les magasiniers doivent trouver un terminal disponible ;

– le nombre de terminaux à disposition des vendeurs, compte tenu qu'on estime que dans 95 % des cas le vendeur doit trouver un terminal disponible ;

© Dunod – La photocopie non autorisée est un délit

– compte tenu des caractéristiques des applications données par le tableau de la figure 19.18, déterminer le temps de réponse de l'application. Les différents éléments à prendre en compte pour ce calcul sont :
  – temps de traitement d'une transaction par le serveur central 0,2 s ;
  – les terminaux sont connectés à un concentrateur local par une ligne à 9 600 bit/s ;
  – le magasin est relié au site central par une liaison louée à 64 000 bit/s
  – on admettra que les bits de transparence et les données de service (ACK...) accroissent la taille des unités de 20 % ;
  – les grilles d'écran des terminaux points de vente sont organisées de telle manière que l'écran de consultation permette de saisir la vente du produit consulté ou la référence d'un autre produit à consulter (un seul échange pour la consultation suivie d'une vente) ;
  – les saisies s'effectuent sur une grille vierge ou en surcharge sur une grille de réponse. Seuls, les caractères saisis sont transmis ;
  – le temps de saisie n'est pas décompté dans le temps de réponse ;
  – le temps d'affichage des écrans sera considéré comme négligeable.

Terminal	Point de vente	Caisse	Point d'enlèvement	Comptable
Saisie	20c	100c	20c	200c
Réponse ou grille de saisie vierge	800c	500c	600c	800c

Figure 19.18 Caractéristiques des transactions.

Exercice 19.3 Réalisation d'un réseau privé d'entreprise

Une entreprise désire réaliser un réseau privé à partir de liaisons louées (LL) à 64 kbit/s pour remplacer ses abonnements à un réseau public de transport de données dont le débit d'abonnement est actuellement de 19 200 bit/s. Le siège est à Paris. Les différentes implantations en province sont : Amiens, Lille, Metz, Nancy, Strasbourg, Rennes, Nantes, La Rochelle, Bordeaux, Toulouse, Clermont Ferrand, Dijon, Lyon, Marseille et Nice. On vous demande :

– De déterminer le réseau primaire (sans tenir compte d'aucune contrainte de débit), vous utiliserez l'algorithme de Kruskal ;
– D'intégrer une contrainte de débit, en garantissant un débit minimal de 19 200 bit/s à chaque site. C'est-à-dire qu'un nœud de concentration ne doit pas concentrer plus de deux sites. De plus, on souhaite que le nombre de bonds soit au maximum de deux pour chaque site ;
– De comparer les coûts des 2 solutions (l'unité sera le km).

Les distances intersites peuvent être obtenues sur le 36 14 code RLS.

Exercice 19.4 Caractéristique mémoire d'un routeur

Un réseau local est interconnecté à un autre réseau via un routeur par une ligne à 64 kbit/s. Plusieurs stations sont connectées sur le réseau local. L'analyse de trafic en arrivée montre que :

– 2 stations ont un trafic vers l'extérieur de 4 paquets/s ;
– 2 stations ont un trafic vers l'extérieur de 2 paquets/s ;

– 3 stations ont un trafic vers l'extérieur de 6 paquets/s ;
– 5 stations ont un trafic vers l'extérieur de 5 paquets/s.

Les arrivées suivent une loi de Poisson. Les paquets, en arrivée, ont une longueur moyenne de 128 octets. On ne tiendra pas compte des données protocolaires. On vous demande de déterminer :

– le taux d'arrivée (λ) ;
– le taux de service du routeur (μ) ;
– l'intensité de trafic ou la charge du système (ρ) ;
– le nombre moyen de paquets dans le routeur ;
– le temps moyen d'attente ;
– le nombre moyen de paquets en attente ;
– le temps de réponse ;
– la taille du buffer d'entrée dimensionnée au plus juste pour ce trafic, celle-ci sera arrondie au ko supérieur ;
– la taille du buffer n'étant plus de longueur infinie, quelle est dans ces conditions la probabilité de rejet d'un nouvel entrant ?

Exercice 19.5 Temps de transit dans un réseau

Le réseau de la figure 19.19 est constitué de liens à 64 kbit/s, il utilise un routage aléatoire, les analyses de trafic montrent que le trafic entrant par le nœud E est en moyenne de 30 paquets par seconde de longueur moyenne de 128 octets. On admettra qu'il n'y a pas d'autre source de trafic dans le réseau. Tout le trafic entrant en E sort en S et se répartit statistiquement comme l'indique la figure 19.19. On vous demande de déterminer le temps de transit moyen d'un paquet dans le réseau.

Lien	Proportion du trafic écoulé
N1-N2	75 %
N2-N4	50 %
N3-N5	25 %

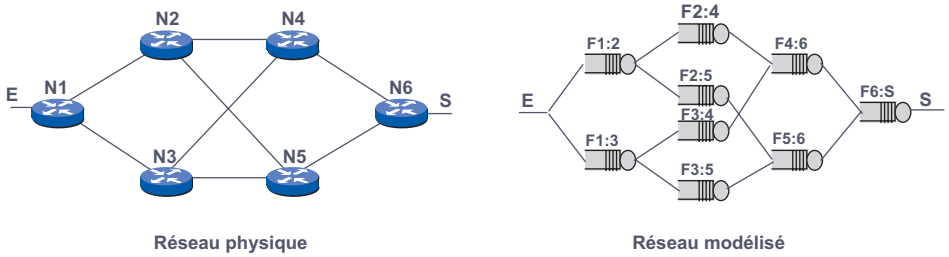


Tableau 19.1 Modélisation du réseau.

© Dunod – La photocopie non autorisée est un délit

Chapitre **20**

Solutions des exercices

CHAPITRE 2

2.1 Code ASCII, Algorithme de changement de casse

Dans le code ASCII, pour passer des majuscules aux minuscules il suffit de rajouter 32 à la valeur du code.

Tant que le caractère actuel n'est pas la marque de fin de chaîne **faire**

```
Début
   | Si le code du caractère n'est pas celui de l'espace alors
   |   |  ajouter 32
   | Finsi
   | passer au caractère suivant
Fin
```

```
While (*chaine1)
  {
   if (*chaine1!=32)
       (*chaine1)+=32;
   chaine1++;
  }
```

2.2 Codage de Huffman

Longueur moyenne du code idéal

L'entropie (H) du système exprime la longueur moyenne du code idéal :

$$H = \sum_{i=1}^{i=n} p_i \log_2 \left(\frac{1}{pi}\right)$$

$$H = -3{,}32\,(0{,}23 \times \log_{10}(0{,}23) + 0{,}09 \times \log_{10}(0{,}09) + 0{,}3 \times \log_{10}(0{,}3) + 0{,}19 \times \log_{10}(0{,}19) \times \log_{10}(0{,}14) + 0{,}05 \times \log_{10}(0{,}05) = 2{,}38 \text{ bits.}$$

Construction de l'arbre de Huffman (figure 20.1)

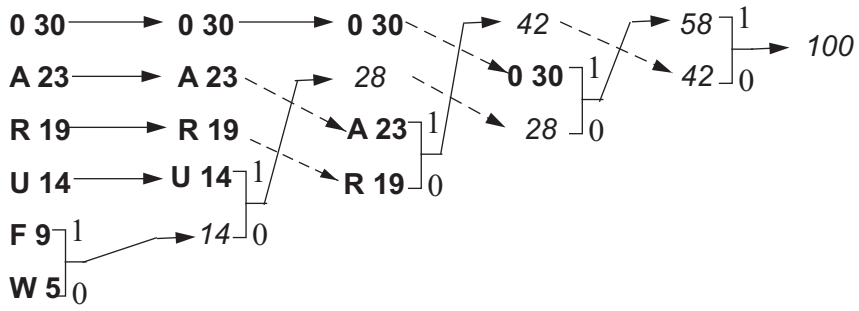


Figure 20.1 Codage de Huffman.

Le codage résultant est **O = 11 ; A = 01 ; R = 00 ; U = 101 ; F = 1001 ; W = 1000.**
Nombre de bits utilisés pour coder le message de 2 000 caractères :

$$2\,000 \times (A \times 0,23 + F \times 0,09 + O \times 0,30 + R \times 0,19 + U \times 0,14 + W \times 0,05)$$

Soit $2 \times 460 + 4 \times 180 + 2 \times 600 + 2 \times 380 + 3 \times 280 + 4 \times 100 = 4\,840$ bits.

Longueur moyenne du mot code

4 840/2 000 = 2,42 bits (remarquons que cette longueur est proche de celle du codage idéal).

Taux de compression par rapport au code Baudot

Le code Baudot est un code de longueur fixe à 5 moments, le taux de compression (τ) vaut $\tau = 2{,}42/5 = 0{,}484$.

Temps de transmission (*t*) du message

– En ASCII (7 bits) : $t = \text{Volume/débit} = 2\,000 \times 7/4\,800 = 2{,}91$ s.
– Codé Huffman : $t = \text{Volume/débit} = 4\,840/4\,800 = 1{,}008$ s.

Remarquons que le temps calculé pour la transmission en Huffman ne prend pas en compte l'envoi du dictionnaire.

2.3 Télécopieur

À partir du tableau de la figure 20.2 établissons les statistiques d'utilisation de chaque groupement de pixels. Pour simplifier la résolution, à chaque séquence de blancs ou de noirs, nous associerons une lettre.

Groupement de	Nb occurrences Blanc		Nb occurrences Noir	
1 pixel	6	A	32	E
2 pixels	14	B	4	F
3 pixels	16	C	5	G
4 pixels			2	H
5 pixels	2	D		

Figure 20.2 Tableau des occurrences d'apparition des groupements de pixels.

Le code de Huffman résultant est déduit de la figure 20.3.

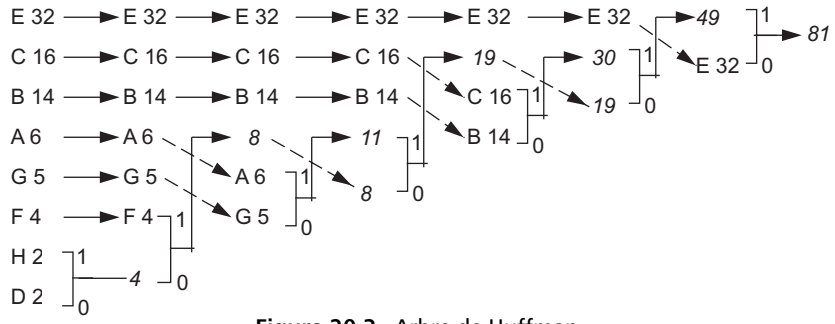


Figure 20.3 Arbre de Huffman.

Pour obtenir le code de Huffman de chaque symbole, il suffit de lire, de la racine à la feuille, les valeurs binaires inscrites. Ces valeurs sont indiquées dans la figure 20.4.

Groupement de	Blancs		Noirs	
1 pixel	1011	A	0	E
2 pixels	110	B	1001	F
3 pixels	111	C	1010	G
4 pixels			10001	H
5 pixels	10000	D		

Figure 20.4 Table de codage.

2.4 Numérisation du son

Débit binaire nécessaire

CD audio : $44{,}1 \cdot 10^3 \times 16 = 705{,}6$ kbit/s ;

DVD audio : $192 \cdot 10^3 \times 24 = 4{,}608$ Mbit/s ;

SACD : $2{,}8224 \cdot 10^6 \times 1 = 2{,}8224$ Mbit/s.

© Dunod – La photocopie non autorisée est un délit

Volume à stoker pour 1 heure de musique

1 kilo-octet(ko) = 1 024 octets ;

CD audio : $705{,}6 \cdot 10^3 \times 3\,600/(8 \times 1\,024) = 310\,078{,}125$ ko = 302 Mo ;

DVD : $4,608 \cdot 10^6 \times 3\,600/8 \times 1\,024) = 2\,025\,000$ ko = 1 0977,53 Mo = 1,9311 Go ;

SACD : $2{,}8224 \cdot 10^6 \times 3\,600/8 = 1\,240\,312{,}5$ ko = 1 211,24 Mo = 1,182 Go.

2.5 Numérisation et débit binaire

Détermination du débit

La fréquence minimale d'échantillonnage étant le double de la fréquence maximale du signal à discrétiser cette fréquence est de :

– Information de luminance (Y) : $F_{\text{echy}} = 6{,}75 \times 2 = 13{,}5$ MHz.

– Informations de chrominance (Db et Dr) : $F_{\text{echc}} = 13{,}5\ \text{MHz}/2$.

Le nombre total d'échantillons quantifiés est de $13{,}5{\cdot}10^6{+}2(13{,}5{\cdot}10^6/2) = 27{\cdot}10^6$ échantillons. En quantifiant chaque échantillon sur 8 bits le débit nécessaire est de $27{\cdot}10^6 \times 8 = 216\ \text{Mbit/s}$.

Nombre de couleurs

Les informations de couleur sont quantifiées sur 8 bits soit 256 niveaux pour chacune des trois primaires. Dans ces conditions le nombre de couleurs reproductibles est de 256^3 soit 16 millions de couleurs.

2.6 Rapport signal à bruit et loi de quantification A

Le signal de base est quantifié dans une représentation logarithmique à 7 segments (ligne 1 du tableau de la figure 20.5). Chaque segment est divisé en 16 intervalles égaux (ligne 2). Cependant, l'amplitude représentée par chaque segment double pour chaque segment, sauf les deux premiers (ligne 3).

Segment	0	1	2	3	4	5	6	7
Codage	0-15	16-31	32-47	48-63	64-79	80-95	96-111	112-127
Amplitude (11bits)	0-15	16-31	32-63	64-127	128-255	256-511	512-1023	1024-2047
Amplitude d'un échelon	16/16 = 1	16/16 = 1	32/16 = 2	64/16 = 4	128/16 = 8	256/16 = 16	512/16 = 32	1 024/16 = 64
Erreur de quantification	0,5	0,5	1	2	4	8	16	32
Signal de référence	8	24	48	96	192	384	768	1536
S/B	16	48	48	48	48	48	48	48

Figure 20.5 Loi de quantification A.

Ainsi, par exemple le segment 5 s'étend sur 256 niveaux (ligne 3) pour un intervalle de définition total de 2 048 échelons (11 bits), l'amplitude de chaque échelon quantifié est donc dans le rapport 256/16 (256 niveaux codés sur 16, ligne 4 du tableau). Si on admet que l'erreur de quantification maximale correspond à un demi-intervalle de quantification, on en déduit que pour les deux premiers segments cette erreur est de 0,5 ; pour le segment 3 elle est de 1... Si on prend comme signal de référence la valeur centrale de chaque segment (ligne 6), on établit la valeur du rapport signal à bruit (ligne 7).

Sans prétendre à la rigueur mathématique, cet exercice illustre de façon simple l'intérêt de la loi de quantification logarithmique qui permet un rapport signal à bruit pratiquement indépendant de l'amplitude du signal.

2.7 Image RVB

La télévision numérique transmet le signal de luminance (Y) en pleine bande (720 points/ligne) et les informations de différence de couleur (Dr et Db) en demi-bande (360 points/ligne). Le nombre de points quantifiés est donc de 1 440 points/ligne. En mode RVB, les détails de l'image sont apportés par chaque information (720 points/ligne). Le nombre de points transmis par ligne est donc 2 160 points/ligne (720×3).

Le mode Y, Dr, Db réalise donc une compression. Le taux de compression[1] (τ) de celle-ci vaut $\tau = 1\,440/2\,160 = 0{,}66$.

CHAPITRE 3

3.1 Organisation des échanges

Le tableau de la figure 20.6 décrit succinctement les modes d'échange et fournit un exemple pour chacun d'eux.

Mode d'échange	Communication	Exemple
Simplex	1 seul sens (diffusion)	Radiodiffusion
Half Duplex	Dans les deux sens successivement	CB (Citizen Band)
Full Duplex	Dans les deux sens simultanément	Téléphone

Figure 20.6 Les modes d'échange.

3.2 Transmission parallèle

Dans une transmission parallèle, lorsque le retour est commun il faut autant de fils que de bits à acheminer plus 1 pour le retour, soit dans notre cas 33 conducteurs. Si le retour n'est pas commun, chaque bit nécessite 2 fils, soit 64 conducteurs.

Une transmission série n'aurait nécessité que 2 conducteurs.

1. Rappelons qu'en toute rigueur, la grandeur « taux de compression » n'a de signification qu'en cas de compression sans perte.

© Dunod – La photocopie non autorisée est un délit

3.3 Transmission synchrone et asynchrone

Lorsque le signal d'horloge de l'émetteur est transmis ou que celui-ci est déduit des données transmises, on parle de transmission synchrone. Sinon, la transmission est dite asynchrone.

3.4 Éléments d'accès au réseau

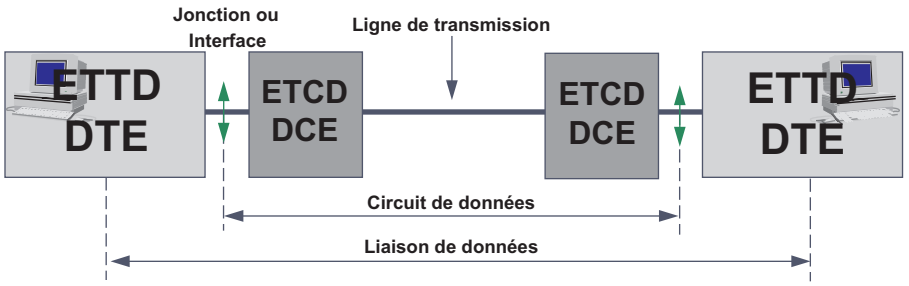


Figure 20.7 Éléments de liaison de données.

La figure 20.7 rappelle le schéma de principe d'une liaison de transmission de données. Le DTE (ETTD) traite les données. Le format électrique de celle-ci n'est pas adapté aux supports de transmission. Il est nécessaire de réaliser une adaptation, c'est le rôle du DCE. Par conséquent, la réponse à la question est non, il est nécessaire d'intercaler un DCE entre le DTE et la ligne.

3.5 Transmission asynchrone

La durée d'un bit correspond à 1 période d'horloge soit 1 ms. Durant cette période l'horloge dérive d'un centième soit $1\ \text{ms} \cdot 10^{-2} = 0{,}01\ \text{ms/période}$. Si la dérive acceptable est de 10 % d'un temps bit, la dérive maximale peut aller jusqu'à $1\ \text{ms} \times 0{,}1 = 0{,}1\ \text{ms}$. Ce qui correspond à Nombre de bits = Dérive maximale/dérive par temps d'horloge, alors Nombre de bits $= 0{,}1/0{,}01 = 10$ bits.

3.6 Temps de transfert d'information

La sauvegarde ne peut avoir lieu que lorsque tous les traitements sont terminés, c'est-à-dire dans le créneau 22 h 00-6 h 00 soit durant une période de 8 h 00.

Durée de la transmission à 2,048 kbit/s

Volume de données : $10 \cdot 10^9 \times 8 = 80 \cdot 10^9$ bits ;

Durée de la transmission : $800 \cdot 10^9/2{,}048 \cdot 10^6 = 390\,625\ \text{s} = 10\ \text{h}\,51\ \text{min}$;

La transmission ne peut se réaliser durant le temps imparti.

Les solutions envisageables

– Disposer d'un raccordement à débit plus élevé et si 2,048 Mbit/s est le débit maximal réalisable sur un raccordement, utiliser plusieurs (2) raccordements en parallèle.

– Ne faire qu'une sauvegarde incrémentielle, c'est-à-dire ne sauvegarder que les données qui ont été modifiées.
– Réaliser la sauvegarde localement sur un support magnétique et transférer le support par voie normale (routière ou autre) au site de backup.

CHAPITRE 4

4.1 Notion de décibel

Le rapport exprimé en décibel de A sur B est donné par la relation :

$$A/B_{dB} = 10 \log_{10}(A/B)$$

Remarquons que si $A = 2B$, on a le rapport $A/B_{dB} = 10 \log_{10}(2/1) = 10 \times 0,3 = 3$ dB.

3 dB est une valeur caractéristique qui représente un rapport de moitié (-3 dB) ou du double (3 dB) des grandeurs comparées. Le tableau de la figure 20.8 fournit les résultats de l'exercice.

Valeur en décibel	Rapport en nombre naturel
3 dB	2
10 dB	log (A/B) = 1 ⇒ A/B = 10 (10^1) Le logarithme d'un nombre est le nombre par lequel il faut élever la base pour retrouver ce nombre.
100 dB	log (A/B)=10 ⇒ A/B = 10^{10}
103 dB	À chaque fois que l'on ajoute 3 dB (100 + 3), on double le rapport soit : 2 * 10^{10}
77 dB	77 dB = 80 – 3 ⇒ A/B = $10^8/2$

Figure 20.8 Grandeurs réelles et décibels.

4.2 Portée d'une liaison hertzienne

Portée théorique

Les faisceaux hertziens utilisent la propagation par onde directe ou propagation à vue. Dans ces conditions la limite de portée correspond au moment où le faisceau est tangent à la Terre (figure 20.9).

Si on ne considère qu'un seul triangle rectangle, on peut écrire :

$$(R+h)^2 = d^2 + R^2 \quad \text{soit} \quad d^2 = (R+h)^2 - R^2 = h^2 + 2Rh$$

avec $h^2 \ll 2Rh$ ($R = 6\,300$ km, et h quelques mètres),

$$d^2 = 2Rh \Rightarrow d = \sqrt{2Rh} = \sqrt{2R}\sqrt{h}$$

alors $d = 3{,}6\sqrt{h}$ avec d en km et h en m.

En posant $P = d_1 + d_2$ on a $P = 3{,}6\left(\sqrt{he} + \sqrt{hr}\right)$ avec P portée optique de la liaison en kilomètres, he et hr hauteur en mètres au-dessus de l'horizon des antennes d'émission et de réception.

© Dunod – La photocopie non autorisée est un délit

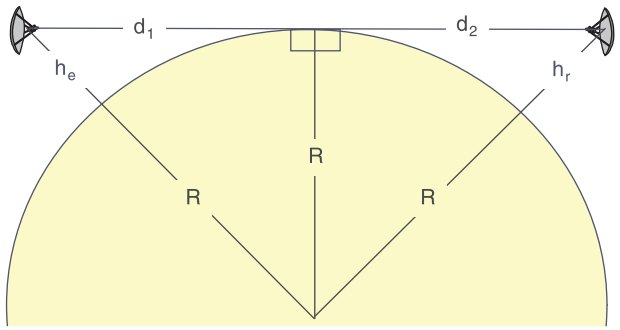


Figure 20.9 Limite de la portée à vue des antennes.

Portée de l'émetteur de la tour Eiffel

La tour Eiffel (312 m) abrite depuis 1956 des antennes d'émission de télévision, celles-ci sont situées à 318 m du sol.

$$P = 3{,}6\left(\sqrt{he} + \sqrt{hr}\right) = 3{,}6\left(\sqrt{318} + \sqrt{10}\right) = 75 \text{ km}$$

4.3 Bande passante d'une fibre optique

Dans une fibre multimode, pour une impulsion émise, N impulsions sont reçues suivants les N trajets empruntés (figure 20.10). Pour distinguer deux bits successifs il faut que les N impulsions du bit précédent soient arrivées. Le temps séparant l'émission de 2 bits successifs doit donc être au minimum égal au temps s'écoulant entre la réception de l'impulsion ayant parcouru le plus faible trajet (I_1) et celle ayant parcouru la plus grande distance (1_n).

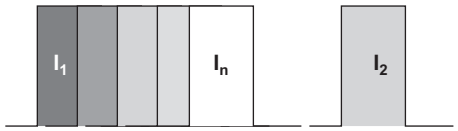


Figure 20.10 Impulsions successives dues aux multiples trajets.

Il faut donc calculer le temps qui sépare l'arrivée des deux impulsions extrêmes (multimode). Pour cela, déterminons la différence de trajet. L'ouverture numérique correspond à l'angle limite des rayons incidents (θ_1), elle permet de calculer le trajet le plus important (figure 20.11).

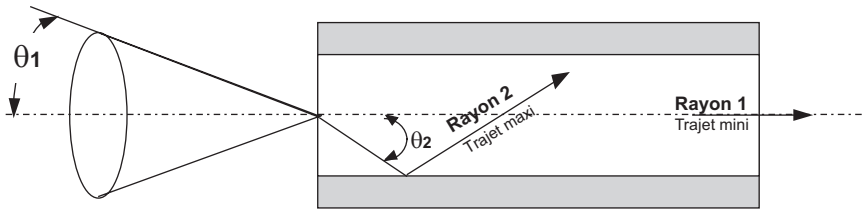


Figure 20.11 Trajets dans la fibre.

Calcul de l'angle de réfraction

L'angle maximal d'acceptance et l'ouverture numérique sont liés par la relation :

$$\text{ON} = \sin\theta_1 \quad \text{or} \quad n_1 \sin\theta_1 = n_2 \sin\theta_2$$

n_1 indice de réfraction de l'air soit 1, n_2 indice de réfraction du cœur de la fibre soit 1,465. Dans ces conditions on peut écrire :

$$\sin\theta_1 = n_2 \sin\theta_2 \quad \text{soit} \quad \sin\theta_2 = \sin\theta_1/n_2 = 0{,}22/1{,}465 = 0{,}150$$

Ce qui donne un angle de réfraction de 8°.

Détermination du trajet maximal

Le trajet parcouru par les rayons R_1 et R_2 sont liés par la relation :

$$R_1 = R_2 \cos\theta_2 \quad \text{d'où} \quad R_2 = R_1/\cos\theta_2$$

Soit, pour un trajet R_1 de 1 km, un trajet $R_2 = 1/\cos\theta_2 = 1\,000/0{,}990 = 1\,010$ m soit une différence de trajet (ΔD) de 10 m.

La différence de temps de trajet (Δt) est de $\Delta t = \Delta D/v$ où v est la vitesse de la lumière dans la fibre optique, $\Delta t = 10/2 \cdot 10^8 = 5 \cdot 10^{-8}$ s.

Calcul de la bande passante

Le temps calculé précédemment représente l'écartement minimal nécessaire (cadence d'émission maximale) entre deux bits du trajet R_1 soit une bande passante maximale de $\text{BP} = 1/5 \cdot 10^{-8} = 20$ Mbit/s.

CHAPITRE 5

5.1 Caractéristiques d'un modem

a) Valence du signal

Un signal à 8 états ou phases et à 2 niveaux par phase correspond à une représentation de 16 valeurs.

b) Rapidité de modulation du signal

La rapidité de modulation envisageable sur le canal est

$$\text{R} = 2 \times \text{BP} = 2 \times (2\,900 - 500) = 4\,800 \text{ bauds}$$

La rapidité de modulation utilisée indique le nombre de changements d'état du signal ; dans le cas présent, 16 états sont possibles par temps élémentaire. Dans ces conditions, si

$$\text{D} = \text{R} \log_2(n)$$

on obtient $\text{R}_{\text{effective}} = \text{Débit}/\log_2(n)$ soit $9\,600/4 = 2\,400$ bauds.

© Dunod – La photocopie non autorisée est un délit

c) Rapport signal à bruit

La capacité de transmission maximale du canal est donnée par la relation de Shannon :

$$C = BP \log_2(1 + S/N)$$

Cependant, pour appliquer cette formule ici, il faut tenir compte non pas de la bande passante réelle du circuit, mais de celle utilisée par le modem, ce qui peut s'écrire :

$$C = (R/2) \log_2(1 + S/N)$$

avec $C_{(capacité)} = 9\,600$ bit/s et $R_{(effective)} = 2\,400$ bauds.

Soit $\log_2(1 + S/N) = 9\,600/1\,200 = 8$ d'où $2^8 = 1 + S/N$ et $S/N = 256 - 1 = 255$.

On aurait pu directement appliquer directement $n = \sqrt{(1 + S/N)}$, ce qui aurait évidemment donné le même résultat. Soit un rapport Signal/Bruit (S/N, Signal/Noise) limite de 255.

5.2 Débit possible sur un canal TV

Rapidité de modulation :

$$R = 2 \times BP$$

$R_{max} = 2 \times 6$ MHz $= 12$ Mbauds. Le canal est susceptible d'admettre une capacité de modulation de 12 Mbauds.

Compte tenu de l'utilisation d'un signal de valence 4, le débit possible est :

$$D = R \log_2(n)$$

Soit $D = 12 \cdot 10^6 \times \log_2(4) = 24 \cdot 10^6$ bit/s.

5.3 Rapport Signal/Bruit

Détermination du rapport Signal/Bruit (ou S/N, Signal/Noise) en dB :

$$S/B_{dB} = 10 \log_{10}(S/N)$$

Soit 30 dB $= 10 \log_{10}(S/N)$ et $\log_{10}(S/N) = 30/10 = 3$.

Le logarithme d'un nombre est le nombre par lequel il faut élever la base pour retrouver ce nombre soit $X = 10^3 = 1\,000$. Le rapport signal sur bruit en grandeur réelle est donc de 1 000.

En appliquant la relation de Shannon :

$$C = BP \times \log_2(1 + S/N)$$

On obtient $C = 3\,100 \times \log_2(1\,000)$ en effet $(1 + 1\,000) \approx 1\,000$.

Pour mémoire rappelons une solution simple de conversion de logarithme en base 10 en logarithme en base 2 :

$$\log_2(x) = \mathrm{N}\log_{10}(x) \quad \text{soit} \quad \mathrm{N} = \log_2(x)/\log_{10}(x)$$

Avec $x = 2$, on a

$$\mathrm{N} = 1/\log_{10} 2 = 1/0{,}30109 = 3{,}32$$

$$\mathrm{C} = 3\,100 \times 3\,32 \times \log_{10}(1\,000) = 3\,100 \times 3{,}32 \times 3 = 30\,876 \text{ bit/s}$$

La capacité maximale théorique du canal est donc de 30 876 bit/s.

5.4 Le Null Modem

Signaux à câbler (figure 20.12)

N° de circuit	Appellation	Fonction
102	Signal Ground (**SG**)	Terre de signalisation ou retour commun
103	Transmitted Data (**TD**)	Circuit par lequel l'ETTD transmet les données à émettre
104	Receive Data (**RD**)	Circuit par lequel l'ETCD transmet à l'ETTD les données qu'il a reçues
105	Request To Send (**RTS**)	Circuit par lequel l'ETTD demande à l'ETCD de se mettre en position de recevoir des données à transmettre.
107	Clear To Send (**CTS**)	En réponse au 105, l'ETCD répond qu'il est connecté à la ligne et prêt à émettre des données.
108	Data Set Ready (**DSR**)	L'ETTD demande à l'ETCD de se connecter à la ligne
109	data Carrier Detect (**CD**)	L'ETCD signale qu'il reçoit un signal (porteuse) conforme à son attente.

Figure 20.12 Signaux à gérer.

Réalisation du câble

La réalisation d'un câble de connexion directe entre deux ETTD n'est pas aussi simple qu'il peut y paraître. En effet, il faut envisager plusieurs modes de fonctionnement et donc plusieurs solutions de câblage. La figure 20.13 représente le cas le plus simple. Dans ce mode de fonctionnement aucun contrôle n'est réalisé, les seuls circuits à câbler sont le 103, 104 (en les croisant) et le 102 (Terre de signalisation).

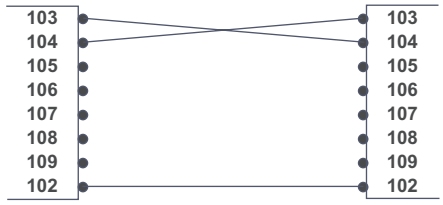


Figure 20.13 Éliminateur de modems.

L'étape suivante consiste à fournir à l'ETTD les réponses qu'il attend de l'ETCD. Pour cela, il faut boucler le 108 et le 107 (réponse au 108) ainsi que le 105 et le 106 (réponse au 105). Reste à résoudre le problème du 109. Le 109 est activé quand l'ETCD reçoit la porteuse du distant. Cette porteuse a été envoyée suite à la levée du 105. Par conséquent, le 105 local sera raccordé au 109 distant (figure 20.14).

© Dunod – La photocopie non autorisée est un délit

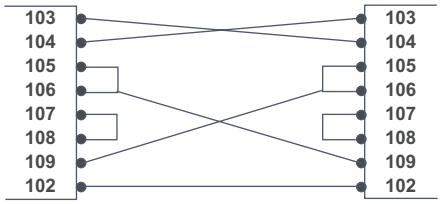


Figure 20.14 Null Modem.

D'autres solutions sont envisageables selon le contrôle de l'interface que l'on désire réaliser. La solution présentée ici n'est qu'une parmi d'autres possibles.

5.5 Contrôle de flux matériel

Lors de l'échange de données entre l'ETTD et l'ETCD, la mémoire tampon (buffer) de l'un ou de l'autre peut être pleine et par conséquent engendrer une perte de données si de nouvelles données sont envoyées. En positionnant les signaux RTS (105, ETTD prêt) et CTS (106, ETCD prêt) à OFF, l'ETTD ou l'ETCD informe l'autre qu'il ne peut plus accepter de données. Cette technique de contrôle du débit à l'interface s'appelle contrôle de flux matériel.

5.6 Modem dissymétrique

1) Rapport signal/bruit

Les tableaux de la figure 20.15 indiquent les éléments générateurs de bruit à prendre en compte dans chaque sens de la liaison :

Usager ⟶ Entreprise	Ligne analogique	Codec	RTPC	Ligne numérique
Entreprise ⟶ Usager	Ligne analogique		RTPC	Ligne numérique

Usager ⟶ Entreprise	$2{\cdot}10^{5}$	$1{\cdot}10^{3}$	$1{\cdot}10^{8}$	$2{\cdot}10^{5}$
Entreprise ⟶ Usager	$2{\cdot}10^{5}$		$1{\cdot}10^{8}$	$2{\cdot}10^{5}$

Figure 20.15 Éléments de la liaison.

a) S/B Usager → Entreprise : $[\mathrm{S/B}]^{-1} = 0{,}5 \cdot 10^{-5} + 10^{-3} + 10^{-8} + 0{,}5 \cdot 10^{-5} = 10^{-3}$

b) S/B Entreprise → Usager : $[S/B]^{-1} = 0{,}5 \cdot 10^{-5} + 10^{-8} + 0{,}5 \cdot 10^{-5} = 10^{-5}$

2) Caractéristiques de la liaison

a) Rapidité de modulation

La bande passante étant la même dans les deux sens, la rapidité de modulation est identique

$$\mathrm{R} = 2 \times \mathrm{BP} = 2 \times 3\,400 = 6\,800 \text{ bauds}$$

b) Débit maximal dans chacun des deux sens

Rappelons que le débit maximal ou capacité du support est fonction de la bande passante et du rapport signal à bruit du lien :

$$\mathrm{C} = \mathrm{BP} \log_2(1 + \mathrm{S/B})$$

Usager → Entreprise : $C = 3\,400 \times 3\,32 \log_{10}(10^3) = 3\,400 \times 3{,}32 \times 3 = 33\,864\,(33\,000)$ bit/s

Entreprise → Usager : $C = 3\,400 \times 3{,}32 \log_{10}(10^5) = 3\,400 \times 3{,}32 \times 5 = 56\,440\,(56\,000)$ bit/s

c) et d) Valence du signal

$D = 2BP \log_2(v)$ et $\log_2(v) = D/(2BP)$

Usager → Entreprise : $\log_2(v) = 33\,000/6\,800 = 4{,}85$ soit MAQ 32

Entreprise→Usager : $\log_2(v) = 56\,000/6\,800 = 8{,}63$ soit MAQ 512

5.7 Rapidité de modulation

Le codage du signal dans un réseau 802.3 est en Manchester (Biphase), ce type de codage se caractérise par une transition au milieu de chaque temps bit, il y a donc deux états par temps bit ; la rapidité de modulation est le double du débit soit 20 Mbauds.

Autre explication : le codage Manchester correspond à un codage nB/mB. En effet, un 0 correspond à l'émission de 01 (niveau électrique) et un 1 correspond à l'émission de 10 (niveau électrique).

La vitesse de signalisation sur la ligne ou rapidité de modulation est bien le double du débit binaire.

CHAPITRE 6

6.1 Calcul de CRC

Le polynôme générateur $x^4 + x^2 + x + 1$

donne la séquence binaire $1(x^4) + 1(x^2) + 1(x^1) + 1(x^0)$ soit 10111.

La division est, en réalité, un OU exclusif qui peut être exécuté dans des registres à décalage. Le degré du polynôme générateur étant de 4, on doit ajouter 4 zéros à la trame de donnée. La division est représentée ci-après. Le résultat n'est pas exprimé, il est sans intérêt, seul le reste de cette division présente une utilité.

```
1 0 1 0 0 1 0 1 1 1 0 0 0 0   | 1 0 1 1 1
1 0 1 1 1                     | 100 110 0100
0 0 0 1 1 1 0 1               | ce quotient est sans intérêt
        1 0 1 1 1
        0 1 0 1 0 1
          1 0 1 1 1
          0 0 0 1 0 1 0 0
                1 0 1 1 1
                0 0 0 1 1 0 0
```

Le reste, de degré $n - 1$ par rapport au polynôme générateur, est exprimé sur 4 bits. Ce reste est de 1100, le CRC4 est donc de 1100. Le message à transmettre sera :

1 0 1 0 0 1 0 1 1 1 **1 1 0 0**

© Dunod – La photocopie non autorisée est un délit

Vérification :

```
message                    reste
1 0 1 0 0 1 0 1 1 1        1 1 0 0  | 1 0 1 1 1
1 0 1 1 1                           |
0 0 0 1 1 1 0 1                     |
      1 0 1 1 1                     |
      0 1 0 1 0 1                   |
          0 0 0 1 0 1    1 1        |
                1 0 1    1 1        |
              0 0 0      0 0 0 0    |
```

6.2 Probabilité de recevoir un message erroné

Si Te est la probabilité pour qu'un bit soit erroné, la probabilité de recevoir un bit correct est de $(1 - \text{Te})$; pour un bloc de N bits la probabilité est de $(1 - \text{Te})^N$. Soit, pour un message de 100 caractères comportant 7 bits/caractère (code CCITT N° 5) : $100 \times 8 = 800$ bits (on transmet des octets en entier).

La probabilité Pc de réception d'un bloc correct est :

$\text{Pc} = (1 - 0{,}0001)^{800} = (0{,}9999)^{800} = 0{,}923.$

La probabilité Pe de recevoir un bloc erroné est :

$\text{Pe} = 1 - 0{,}923 = 0{,}077$

6.3 Taux de transfert

a) Taux de transfert d'information sans erreur

L'efficacité du protocole sans erreur est :

$$\text{E}_{\text{ff}} = \text{ Nb bits utiles/Nb bits transmis}$$

Nombre de bits utiles $= 1\,000 \times 7 = 7\,000$ bits (code CCITT N° 5 codé sur 7 bits).

Nombre de bits transmis $= 1\,000 \times (7 + 1) = 8\,000$ bits (7 pour 1 car + 1 bit de parité) alors $\text{E}_{\text{ff}} = 7\,000/8\,000 = 0{,}875$.

Le taux de transfert d'information (TTI) est :

$$\text{TTI} = \text{Débit théorique } \times \text{ Efficacité}$$

Soit $\text{TTI} = 9\,600 \times 0{,}875 = 8\,400$ bit/s.

b) Taux de transfert d'information en milieu erroné

En milieu erroné, l'efficacité du protocole est le produit de l'efficacité sans erreur et de la probabilité de réception correcte du message. La probabilité de recevoir un message correct de N bits pour un taux d'erreurs de Te :

$$\text{P} = (1 - \text{Te})^N$$

Soit $\text{P} = (1 - 0{,}0001)^{8\,000} = 0{,}9999^{8\,000} = 0{,}449$.

Le taux de transfert avec erreurs est :

$$\text{TTI}_{\text{avec erreur}} = \text{TTI}_{\text{sans erreur}} \times \text{P}$$

Soit $\text{TTI}_{(\text{avec erreur})} = 8\,400 \times 0{,}449 = 3\,770$ bit/s.

6.4 Échange HDLC version LAP-B

Le tableau de la figure 20.16 représente l'échange, les commentaires nécessaires à la compréhension de chaque échange sont fournis à la ligne correspondante.

	A		Échange	B	
Valeur des compteurs après l'échange (après émission et après réception)	Vs	Vr		Vs	Vr
Exemples de représentation des trames : Indiquer le type (I, U, S) Éventuellement la trame (REJ, SABME…) Les valeurs des compteurs Nr, Ns La valeur du bit P/F			(I) Ns = 4 Nr = 6 P = 0 ⟶ (S) RNR Nr = 3 P = 0 ⟵		
Initialisation :	0	0		0	0
1) Ouverture en mode asynchrone normal	0	0	(U) SABM P = 0 ou 1 ⟶	0	
2) Acceptation par B	0	0	(U) UA F = 0 ou 1 ⟵	0	0
Échange :					
3) Trame d'information de A vers B	1	0	(I) Ns = 0, Nr = 0 P= 0 ⟶	0	1
4) Trame d'information de A vers B erronée	2	0	(I) Ns = 1, Nr = 0 P = 0 ⟶ *non prise en compte*	0	1
5) Trame d'information de A vers B	3	0	(I) Ns = 2, Nr = 0 P = 0 ⟶ *rejet décalage des compteurs*	0	1
6) *La trame précédente à été rejetée* *Demande de retransmission*	3	0	(S) REJ Nr = 1 P = 0 ⟵	0	1
7) Trame d'information de A vers B	2	0	(I) Ns = 1, Nr = 0 P = 0 ⟶	0	2
8) Trame d'information de A vers B	3	0	(I) Ns = 2, Nr = 0 P = 0 ⟶	0	3
9) Trame d'information de B vers A	3	1	(I) Ns = 0, Nr = 3 P = 0 ⟵	1	3
10) Trame d'information de A vers B	4	1	(I) Ns = 3, Nr = 1 P = 0 ⟶	1	4
11) Trame d'information de A vers B	5	1	(I) Ns = 4, Nr = 1 P = 0 ⟶	1	5
12) Trame d'information de A vers B	6	1	(I) Ns = 5, Nr = 1 P = 0 ⟶	1	6
13) Trame d'information de A vers B	7	1	(I) Ns = 6, Nr = 1 P = 1 ⟶	1	7
14) *Envoi d'un acquittement*	7	1	S) RR Nr = 7 F = 1 ⟵	1	7
Fermeture de la connexion :					
15) Demande de fermeture			(U) DISC P = 1 ⟶		
16) Acquittement par B			(U) UA F = 1 ⟵		

Figure 20.16 Échange LAP-B.

© Dunod – La photocopie non autorisée est un délit

CHAPITRE 7

7.1 Intensité de trafic et taux d'activité

Lors de l'étude d'un système d'interconnexion de systèmes informatiques, deux critères essentiels, dépendant du type d'application, sont à prendre en compte :

– l'intensité de traffic qui caractérise la durée de la ou des sessions ;

– le taux d'activité, qui exprime la proportion de temps d'utilisation pendant le temps de connexion.

L'intensité de trafic (E) et le taux d'activité (θ) varient de 0 à 1. On peut représenter la relation entre ces valeurs par un rectangle et déterminer 4 aires spécifiques (figure 20.17).

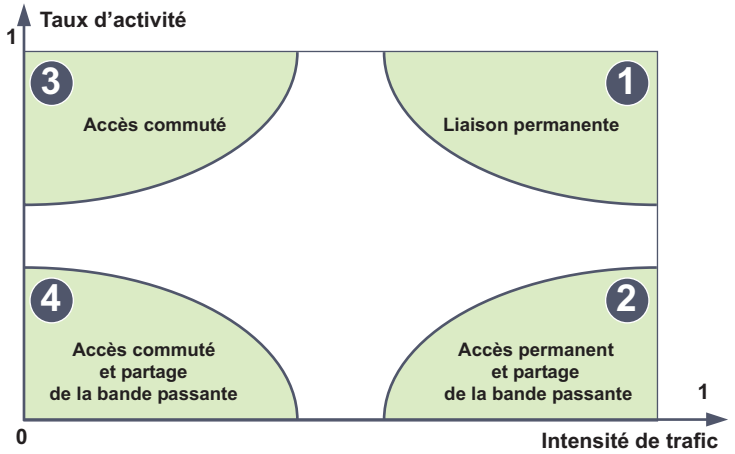


Figure 20.17 Les 4 aires définies par E et θ.

– L'aire 1 correspond à une occupation de la ligne importante et une utilisation conséquente, le partage des ressources n'est pas envisageable.

– L'aire 2 correspond aussi à une occupation de la ligne importante, mais à une utilisation faible. La bande passante de la ligne peut donc être partagée, le multiplexage est envisageable.

– L'aire 3 représente un secteur ou la ligne est peu occupée, mais le trafic est important. Le partage de la bande n'est pas envisageable, mais le partage dans le temps de son utilisation est possible. La ligne peut être commutée d'un utilisateur à un autre (réseaux à commutation de circuits).

– Dans la dernière aire, la ligne est peu occupée et faiblement utilisée, on peut imaginer un système de concentration de trafic auquel on accède via un réseau commuté, ce système servant d'interface avec un autre moyen où la bande pourra statiquement être partagée par plusieurs utilisateurs.

Le tableau de la figure 20.18 résume ces commentaires.

Intensité de trafic (E)	Taux d'activité (A)	Commentaires		Service	Type d'application (exemples)
Voisin de 1	**Voisin de 1 Aire 1**	La ligne est occupée en permanence	La bande est totalement utilisée, tout partage est impossible	LS	Télémesure, Conduite de processus
	Faible Aire 2	une liaison permanente est nécessaire	La bande offerte est peu utilisée, son utilisation peut être partagée	– Réseau de transmission de données – en local multiplexage concentrateur	Système transactionnel (réservation…), Réseau bancaire
Faible	**Voisin de 1 Aire 3**	La ligne est faiblement occupée, il n'est pas nécessaire de disposer d'une liaison permanente	Durant l'utilisation de la ligne, la bande est intégralement occupée par le terminal ; aucun partage n'est envisageable	Réseau téléphonique	Transfert de fichiers
	Faible Aire 4	un service de commutation est envisageable	Durant l'utilisation du média, toute la bande n'est pas occupée, une double concentration est envisageable	Accès téléphonique à un réseau de transmission de données	Minitel

Figure 20.18 Rationalisation des moyens.

7.2 Application numérique E et θ

a) L'intensité du trafic de la ligne

$$E = NT/3\,600 = 1 \cdot 10/60 = 0.166 \text{ erlang}$$

b) Le taux d'activité de la ligne

$$\theta = (n \times L)/(D \times T)$$

n = nombre de messages échangés durant la session

L = longueur moyenne des messages exprimée en bits

D = débit effectif du système

T = durée de la session en s

Le taux d'activité de la ligne est donc $\theta = (1 \times 120\,000 \times 8)/(2\,400 \times 600) = 0.666$.

c) Type d'application

Le taux d'activité est important alors que le taux de connexion est faible. Cette application pourrait être un transfert de fichiers utilisant le réseau téléphonique commuté (RTC, 2 400 bit/s).

7.3 Trame MIC

a) Période de la trame MIC

La trame MIC est reproduite 8 000 fois par seconde (8 000 Hz) soit une période de 125 µs.

© Dunod – La photocopie non autorisée est un délit

b) Débit binaire

La voix est quantifiée sur 256 niveaux soit 8 bits. Le débit, pour une voie, est donc de $8\,000 \times 8 = 64$ kbit/s.

c) Fréquence de récurrence

Le motif se reproduit 1 fois toutes les 16 trames, soit $8\,000/16 = 500$ Hz.

d) Bande allouée

La bande allouée est donc de $500 \times 4 = 2$ kbit/s.

7.4 Multiplexeur

a) Longueur de l'IT

La longueur de l'IT, exprimée en bits, correspond à l'ensemble des informations nécessaires à la reconstitution d'un échantillon du signal. Celui-ci étant quantifié sur 256 niveaux, chaque échantillon contiendra 8 bits ($2^8 = 256$). La longueur de l'IT en tenant compte du bit de signalisation est donc de 8 bits.

b) Rythme et longueur de la trame

Pour assurer un débit de 64 000 bit/s par IT de 8 bits et 1 IT par trame, il faut $64\,0000/8 = 8\,000$ IT pour chaque voie soit 8 000 trames/s.

Compte tenu de l'IT de synchronisation chaque trame écoule 32 IT(30 + 2) soit une longueur de trame, exprimée en bits de $32 \times 8 = 256$ bits.

c) Débit du lien composite

Sauf pour les multiplexeurs statistiques, le débit composite (D_c) d'un multiplexeur doit être au moins égal à la somme des débits des voies basse vitesse (D_{bv}), le débit à écouler est de :

$$D_c = \sum D_{bv}$$

Soit $D_c = 32 \times 64\,000 = 2\,048$ kbit/s.

d) Efficacité du multiplexeur

L'efficacité du multiplexeur est le rapport entre le débit utile écoulé sur la voie composite et le débit du lien. Le débit utile correspond aux 30 IT de voix, l'efficacité est alors de $E = 30/32 = 0,9375$ soit 94 %.

CHAPITRE 8

8.1 Évaluation du nombre de liaisons

Pour un réseau de $n - 1$ nœuds complètement interconnectés, il faut, pour interconnecter le $n^{\text{ème}}$ nœud, $(n - 1)$ liaisons. Soit pour les n nœuds du réseau n $(n - 1)$ liaisons. Cette manière de compter dénombre 2 fois la même liaison : A → B et B → A. Le nombre de liaisons (N) est donc :

$$N = n(n - 1)/2$$

Pour 100 équipements, $N = 100 \times 99/2 = 4\,950$ lignes.

8.2 Table de routage

Matrice de routage (figure 20.19)

$$M = \begin{bmatrix} 0 & 7 & 0 & 0 & 0 & 4 \\ 7 & 0 & 3 & 0 & 2 & 0 \\ 0 & 3 & 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 & 7 & 4 \\ 0 & 2 & 0 & 7 & 0 & 3 \\ 4 & 0 & 0 & 4 & 3 & 0 \end{bmatrix}$$

de \ à	A	B	C	D	E	F
A	0	7	0	0	0	4
B	7	0	3	0	2	0
C	0	3	0	5	0	0
D	0	0	5	0	7	4
E	0	2	0	7	0	3
F	4	0	0	4	3	0

Figure 20.19 Matrice de routage.

Rappelons que la matrice de routage indique le coût (métrique) d'un lien entre deux nœuds (figure 12.15). Une table de routage est un ensemble de quadruplets :
<Nœud origine, Destination, Nœud suivant, Coût>

- Nœud d'origine ⇒ dénomination de la table ;
- Destination ⇒ ensemble de lignes de la table ;
- Nœud suivant ⇒ ensemble de colonnes qui désigne les successeurs du nœud ;
- Coût ⇒ valeur lue à l'intersection rangée/colonne.

La lecture de la table permet à un paquet de trouver la route à prendre pour rejoindre sa destination. Elle établit une correspondance entre l'adresse destinataire, contenue dans le paquet, et les nœuds voisins. Le choix du nœud voisin peut être unique, ou multiple, selon la politique de routage mise en œuvre.

Arbre de coût minimal du nœud B (figure 20.20)

Routes validées	Routes découvertes	Routes en attente
B,0	BA,7 (en attente, ➡) BC,3 (en attente, ➡) BE,2 (Validée)	BA,7 BC,4
BE,2	EF,5 (en attente, ➡) ED,9 (en attente ➡)	EF,5 ED,9 BA,7 BC,3
BC,3	CD,8 (en attente ➡) ED,9 (Fin, on sait maintenant aller en D pour 8)	CD,8 EF,5 BA,7
EF,5	FA,9 (Fin, on sait déjà aller en A pour 7) FD,9 (Fin, on sait déjà aller en D pour 8)	CD,8 BA,7
BA,7	AF,11 (Fin on sait déjà aller en F pour 5)	CD,8
CD,8	DC,13 (Fin, on sait déjà aller en C pour 3) DE,15 (Fin, on sait déjà aller en E pour 2) DF,12 (Fin, on sait déjà aller en F pour 5)	Vide

© Dunod – La photocopie non autorisée est un délit

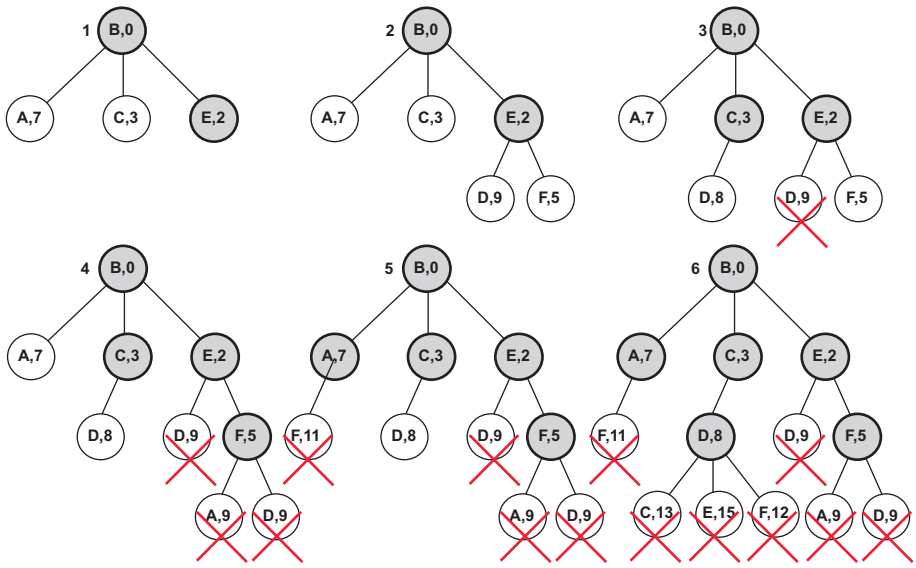


Figure 20.20 Arbre de coût minimal du nœud B.

Ce qui correspond à la table de routage de la figure 20.21 :

Nœud Destination	Nœud Suivant	Coût total
A	A	7
B	Local	0
C	C	3
D	C	8
E	E	2
F	E	5

Figure 20.21 Table de routage du nœud B.

Cartographie du réseau

La cartographie est déduite par simple lecture des liens dans la matrice de routage. La figure 20.22 décrit les différentes étapes.

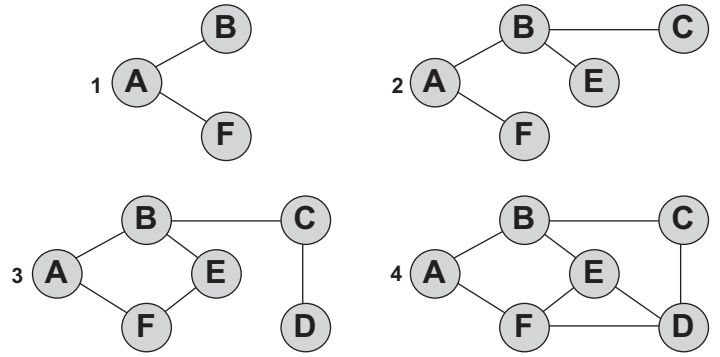


Figure 20.22 Cartographie du réseau.

La lecture de la matrice de routage à partir du nœud A montre qu'on peut atteindre les nœuds B et C (1), de B on joint E et C (2), de C on accède à D, enfin de D on rejoint E et F. L'analyse des nœuds E et F n'apporte aucune connaissance nouvelle.

8.3 Temps de transfert sur un réseau

Taille des unités de données

Le MTU correspond à la taille maximale d'une unité de données du niveau réseau (données du protocole comprises). C'est aussi la charge utile du protocole de niveau liaison. La charge utile du bloc émis par le LAN est donc de $1\,500 - 20 = 1\,480$ octets, ce qui correspond à la taille du message à transmettre.

En commutation de circuits et en commutation de messages, le bloc de données issu du LAN est directement encapsulé dans une unité de données du protocole de liaison ; seul un en-tête de 8 octets est rajouté. L'unité de données à transmettre est donc de $1\,500 + 8 = 1\,508$ octets.

En commutation de paquets et en mode datagrammes, l'en-tête de niveau réseau est recopié dans chaque datagramme. Le tableau de la figure 20.23 fournit, en fonction des MTU respectifs, la charge utile effective et le nombre de datagrammes.

MTU	CU (Charge Utile)	Nombre de paquets 1 480/CU	Taille de l'en-tête H = Hn + Hl
57	37	40	28
168	148	10	28
316	296	5	28

Figure 20.23 Détermination de la charge des paquets.

Pour résoudre ce problème, nous utiliserons la formule générale :

$$Tp = \left(\frac{L + pH}{D}\right)\left(1 + \frac{N}{p}\right)$$

Tp temps de traversée du réseau — L longueur du message
p nombre de paquets — H taille des en-têtes
N nombre de nœuds

a) Temps de transfert en Commutation de Circuits

Pour le message en CC N = 0, p = 1 et l'en-tête vaut Hcc = Hn + Hl = 28 octets donc

$$\text{Tc} = (1\,480 + 28) \times (8/64\,000) = 0{,}1885 \text{ s.}$$

b) Temps en Commutation de Messages

En CM N = 5, p = 1 donc $[(1\,480 + 28) \times (8/64\,000)](1 + 5) = 1{,}131$ s.

© Dunod – La photocopie non autorisée est un délit

c) Temps en Commutation de Paquets

Avec N = 5, H = 28, le temps de transfert est :

– Pour CU 37 : $[(1\,480 + 40 \times 28)(8/64\,000)](1 + 5/40) = 0{,}325 \times 1{,}125 = 0{,}365$ s ;

– Pour CU 148 : $[(1\,480 + 10 \times 28)(8/64\,000)](1 + 5/10) = 0{,}22 \times 1{,}5 = 0{,}33$ s ;

– Pour CU de 296 : $[(1\,480 + 5 \times 28)(8/64\,000)](1 + 5/5) = 0{,}2025 \times 2 = 0{,}405$ s.

De manière générale, plus le paquet est de petite taille meilleur est le temps de transfert. Ce principe a déjà été vu lors de l'étude des multiplexeurs. Cependant en commutation de paquets (multiplexage par étiquette), on ajoute à chaque unité de données un en-tête, de ce fait il existe un rapport harmonieux entre la taille des unités de données et la taille de l'en-tête.

CHAPITRE 9

9.1 Fonctions et couches OSI

a) Le niveau physique réceptionne un flux de bits et le formate en trame pour remise à la couche liaison de données.

b) Le chemin à travers le réseau est déterminé par la couche réseau.

c) La synchronisation des échanges de données est gérée par la couche session.

9.2 Adresse SAP d'une émission FM

Le point d'accès à une entité réseau est la caractéristique qui identifie, sans confusion possible (adresse), un service. Une station d'émission d'un réseau de radio de diffusion est identifiée par sa fréquence d'émission. Le SAP d'une station est sa fréquence d'émission.

Il ne faut pas confondre la NSAP qui identifie le point d'accès à un service réseau avec la SNAP qui identifie le point d'accès au sous-réseau physique de transport, par exemple une adresse X.121.

9.3 Encapsulation

Dans le modèle OSI, ce sont les paquets qui encapsulent les TPDU (figure 20.24). Quand une TPDU arrive au niveau de la couche réseau, la totalité de l'en-tête et des données constituent le champ de données du paquet (N_SDU).

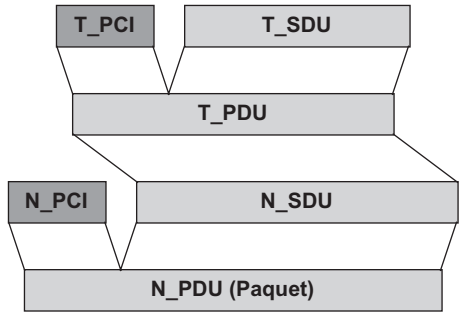


Figure 20.24 Encapuslation des messages de transport.

9.4 Mode connecté et mode non connecté

C'est à partir des fonctionnalités de chacun des modes de mises en relation et des services de chacune des couches que l'on peut définir le mode de mise en relation le mieux approprié pour telle ou telle couche (figure 20.25).

CRITERES	MODE CONNECTE	MODE NON CONNECTE
Etablissement	Oui	Non
Contrôles : **– erreurs** **– flux** **– séquencement**	 Oui Oui Oui	 Non Non Non
Adressage	À l'établissement	Dans chaque entité
Négociation des options	Oui	Non
Type de service	Fiable	Non fiable

Figure 20.25 Synthèses des fonctionnalités selon le mode de mise en relation.

Couche transport

Cette couche a essentiellement pour fonction de rendre le service réseau transparent aux couches de traitement, quelle que soit la qualité du sous-réseau de transport utilisé. De ce fait, c'est elle qui a en charge la correction des erreurs pouvant subsister et la délivrance des messages dans le bon ordre. Cette couche dite de bout en bout a aussi la charge de s'assurer que les données émises peuvent être reçues (contrôle de flux de bout en bout). Dans ces conditions, un service connecté est requis.

Couche réseau

Cette couche doit assurer le routage des paquets à travers un réseau, tous les types de services peuvent être imaginés selon la politique de routage mise en œuvre (aléatoire ou déterministe). Les services en mode non connecté ou connecté sont envisageables.

Couche liaison

Cette couche est la première couche au-dessus du système physique. Si les erreurs « physiques » sont nombreuses, il convient de les corriger au plus vite (reprise sur temporisation ou Nack plus efficace). Ici, un service en mode connecté s'impose. Par contre, si le taux d'erreur est faible, un service non connecté peut être envisagé. La reprise sur erreur dans ce cas pouvant être effectuée par la couche transport (cas des réseaux locaux par exemple).

9.5 Terminal virtuel

Le protocole de terminal virtuel permet aux applications orientées présentation (ex. : les éditeurs) de travailler avec un grand nombre de terminaux incompatibles (interopérabilité). L'émulation « transforme » le terminal réel en terminal du système que l'on émule.

© Dunod – La photocopie non autorisée est un délit

9.6 Contrôle de flux et transferts isochrones

Le mécanisme de contrôle de flux consiste à ralentir, voire arrêter l'émission, la conséquence directe est un asynchronisme dans la réception des données. Cet asynchronisme est incompatible avec une transmission de données dite isochrone comme le nécessite la voix et l'image animée.

9.7 Contrôle de flux et classe de transport 0

Les différentes classes de transport ont été définies pour pallier les insuffisances des sous-réseaux de transport utilisés. La couche transport rend transparent, aux services de session, le sous-réseau physique utilisé. Dans ces conditions, compte tenu que la classe 0 est faite pour s'appuyer sur un service réseau « parfait » elle implémente un minimum de mécanismes. Les TPDU ne comportent pas de champ numéro de TPDU, un service de fenêtrage n'est donc pas réalisable. Le contrôle de flux peut, éventuellement, être effectué par les couches inférieures.

9.8 Référencement d'une connexion de transport

TP4 peut définir des connexions multiples entre toutes les paires de T_SAP. Dans ce cas, les connexions sont identifiées par les champs source référence et destination référence dans les T_PDU et non par l'adresse T_SAP. (Remarquons que dans la TPDU_CR le champ « référence destination » est toujours à zéro.)

9.9 Connexion de transport et connexion de session

Les principales similitudes sont :

– Service orienté connexion.

– Établissement et libération des connexions, avant et après utilisation.

– Primitives de transfert régulier de données.

– Délivrance de données fiables.

Les différences sont :

– La session : libération brutale ou négociée, transport : libération brutale uniquement.

– La connexion de transport n'autorise que des flux de données normales et exprès, la session comporte 4 types de flux de données (voir exercice suivant).

– Les connexions « session » ont un dialogue de gestion, les connexions « transport » un dialogue de transfert.

– Pas de notion de synchronisation, d'activité, ni de jeton dans les connexions transport.

– Une connexion session peut utiliser plusieurs connexions transport.

9.10 Les types de variables d'ASN-1

L'ASN–1 est un langage de description de données. Il définit des types simples ou structurés (comme tous les langages de haut niveau) ; l'ASN–1 est proche, en cela, du langage de programmation PASCAL.

BOOLEAN Représente un type de variable à deux états.

BIT STRING Définit un type de chaîne de caractères binaires. A une chaîne de caractères on associe un chiffre binaire ex : '100011'B .

ISO646STRING Est un identificateur d'objet construit, la première valeur identifie l'organisme de normalisation, la seconde la norme, la troisième le type, ici string (chaîne de caractères).

CHOICE Modélise une variable parmi une collection, chaque élément étant associé à une étiquette spécifique.

SEQUENCE Représente une collection d'objets ordonnés de même type (SEQUENCE, tableau), ou de type différent (SEQUENCE OF, record ou enregistrement).

Le type SET ou SET OF est de nature identique au type SEQUENCE ou SEQUENCE OF. La structure SEQUENCE impose une délivrance ordonnée des données au destinataire. La structure SET autorise une délivrance désordonnée.

IMPLICIT est utilisé quand il n'est pas utile de transmettre le type, le récepteur pouvant le reconnaître

OPTIONAL le champ ne sera transmis que s'il est utile à la transaction en cours

DEFAULT permet d'initialiser une variable

NULL un champ de ce type n'est pas transmis

Prenons, par exemple, la description d'un enregistrement identifiant un compte bancaire :

– Le titulaire du compte est identifié par une chaîne de 20 caractères (champ nom).
– Le code confidentiel d'accès ne sera jamais transmis, il ne peut être utilisé que localement (champ code).
– Le solde du compte, ne sera transmis que s'il est utile à l'opération en cours (champ solde).
– L'autorisation de découvert n'est jamais implicite, le champ est initialisé à FALSE (champ découvert).

Soit la structure :

```
compte : : = IMPLICIT  SEQUENCE
             {
              nom[0]          IMPLICIT OCTET STRING, -- 20 caracteres
              code[1]         IMPLICIT INTEGER NULL,
              solde[2]        IMPLICIT REAL OPTIONAL,
              decouvert[3]    IMPLICIT BOOLEAN DEFAULT FALSE
             }
```

© Dunod – La photocopie non autorisée est un délit

CHAPITRE 10

10.1 Masque de sous-réseau

a) et b) Classe d'adressage

Comme on doit pouvoir adresser 10 sous-réseaux, il faut donc 10 adresses IP dérivées de l'adresse initiale. La valeur décimale 10 se code par 1010 en binaire, il faut donc disposer de 4 bits. Le masque de sous-réseau à construire est donc

```
11111111.11111111.11111111.11110000
```

soit encore

```
255.255.255.240
```

La valeur binaire du premier octet permet de définir la classe d'adressage

```
196D = 1100 0100B,
```

soit une classe C (110)

Autre solution admissible : la classe C couvre les adresses

```
192.0.0.1   à   223.255.255.254
```

c) Machines et sous-réseau

Compte tenu des bits affectés au masque de sous-réseau, il reste 4 bits pour identifier les machines, la valeur 0 représentant le sous-réseau lui-même, la valeur tout à 1 représente l'adresse de broadcast, chaque sous-réseau ne pourra comporter que 14 machines au maximum.

d) Adresse de broadcast du sous-réseau 3

L'adresse de broadcast correspond à tous les bits du champ Host_ID à 1, soit pour le sous-réseau 3, en ne considérant que le dernier octet

```
0011 1111
```

où le premier quartet désigne le sous-réseau 3, le second désignant le Host_ID a tous ses bits à 1. Ce qui, pour cet octet, correspond en décimal à 63, soit l'adresse de diffusion :

```
196.179.110.63.
```

Attention : Il n'y a pas ambiguïté dans l'affectation de la valeur du sous-réseau, la valeur 0 n'étant jamais utilisée pour des raisons de compatibilité. En effet, une vieille version de UNIX considère le champ à zéro comme étant l'adresse de diffusion (UNIX BSD).

10.2 Masque de sous-réseau et dysfonctionnement (figure 20.26)

Source Destination	150.150.1.28 (255.255.255.0)	150.150.1.57 (255.255.0.0)	150.150.2.28 (255.255.255.0)	150.150.2.57 (255.255.0.0)
150.150.1.28		oui	non	oui
150.150.1.57	oui		non	oui
150.150.2.28	non	oui		oui
150.150.2.57	non	oui	oui	

Figure 20.26 Matrice de communication.

10.3 Table ARP

a) Net_ID du réseau

En classe A, le Net_ID est exprimé sur 1 octet, soit dans cet exercice la valeur 10 (adresses privées de classe A).

b) Masque de sous-réseau pour distinguer deux sous-réseaux

Pour distinguer le nombre de bits nécessaires, il suffit d'examiner la valeur binaire du 1er octet du Host_ID, si cela est insuffisant du second... jusqu'à trouver la combinaison binaire qui réponde au problème posé (figure 20.27).

L'examen du tableau ci-contre montre que seuls deux bits sont nécessaires pour distinguer dans le plan d'adressage donné les deux sous-réseaux. Le masque de sous réseau correspondant est `255.192.0.0`.

Station	1er octet du Host_ID	Sous-réseau
99	**01** 100011	SR1
163	**10** 100011	SR2
189	**10** 111101	SR2
126	**01** 111110	SR1

Figure 20.27 Détermination des sous-réseaux.

c) Masque de sous-réseau pour identifier quatre sous-réseaux

La plus petite combinaison binaire pour distinguer quatre sous-réseaux distincts dans les adresses données est de 4. Le masque de sous-réseau est alors `255.240.0.0`.

d) Adresse IP des deux sous-réseaux

L'adresse réseau de chacun des deux sous-réseaux constitués est :

10D.01000000B.0D.0D
10D.10000000B.0D.0D

Notation provisoire utilisée pour indiquer comment sont déterminées les adresses réseaux, D signifie Décimal, B binaire, soit en notation décimale pointée :

10.64.0.0 masque 255.192.0.0
10.128.0.0 masque 255.192.0.0

La figure 20.28 illustre le réseau.

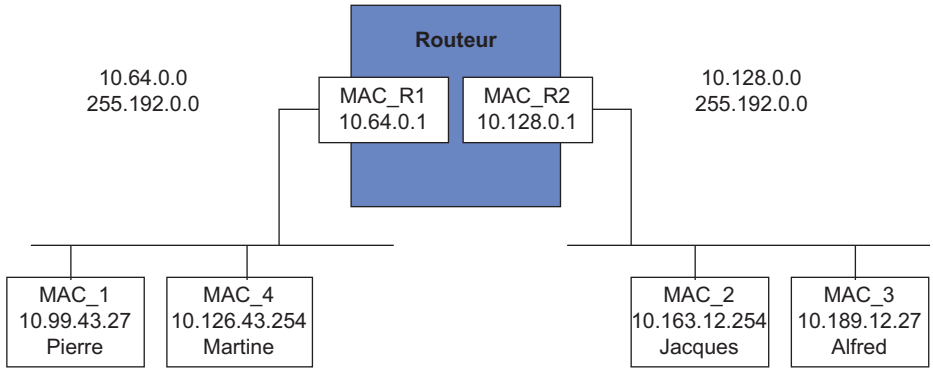


Figure 20.28 Schéma du réseau.

© Dunod – La photocopie non autorisée est un délit

e) Table ARP de la station de Pierre

La table ARP de la station de Pierre est (figure 20.29) :

@IP	@MAC
10.126.43.254	MAC_4
10.163.12.254	MAC_R1
10.189.12.27	MAC_R1

Figure 20.29 Table ARP de la station de Pierre.

f) Accès à Internet

L'entreprise utilise l'adresse 10 qui est une adresse non routable sur Internet. Elle devra faire la demande d'attribution d'adresses officielles. Si elle ne veut pas avoir à revoir la configuration de toutes ses machines, elle devra mettre en œuvre un translateur d'adresses pour avoir accès à Internet (NAT).

10.4 Trace TCP/IP

Généralités

a) Notion d'analyseur

Avant d'examiner la trace de l'exercice, il convient de dire quelques mots sur les appareils qui permettent de les obtenir : les analyseurs. Un analyseur de protocoles est un outil qui permet d'ausculter le réseau. Il permet d'effectuer :

– La mesure des performances du réseau (statistiques).
– De générer un trafic en vue, par exemple, de déterminer des seuils de dysfonctionnement, de tester des évolutions de version de logiciel...
– D'horodater les messages et de déterminer, ainsi, les temps inter-évenements.
– De filtrer certains événements particuliers, par exemple des demandes de connexion...
– D'effectuer des tests et de réaliser la mise au point des protocoles.

Il existe deux types d'analyseurs, les analyseurs WAN et les analyseurs LAN :

– Les analyseurs WAN sont utilisés dans les réseaux WAN, sur une liaison de données, au niveau d'une jonction ETTD/ETCD. Les analyseurs WAN se connectent en mode passif ou actif. Dans le mode passif ou espion ils surveillent le trafic de la station sans en perturber le fonctionnement. En mode actif, ils simulent un ETTD, auquel ils se substituent pour tester le fonctionnement d'un ETCD (ou réseau).
– Les analyseurs LAN sont utilisés dans les réseaux locaux, ils se connectent comme n'importe quelle station et interceptent toutes les informations circulant sur le réseau. Les analyseurs LAN peuvent générer un trafic afin de déterminer les performances du réseau.

En principe un analyseur peut indifféremment être utilisé sur un LAN et sur un WAN. Ce sont les programmes d'analyse et les interfaces physiques qui distinguent les deux fonctionnalités d'un analyseur. Le tableau de la figure 20.30 compare ces deux modes de fonctionnement des analyseurs.

Critères de comparaison	Analyseur WAN	Analyseur LAN
Raccordement	Au niveau de la jonction ETCD/ETTD, la connexion nécessite l'ouverture momentanée de la jonction.	Le raccordement est identique à celui d'une station. La mise en service d'un analyseur LAN ne perturbe pas le réseau.
Vitesse de fonctionnement	Débit actuellement limité à 256 kbit/s.	Conformément aux débits en vigueur sur les réseaux locaux, les analyseurs LAN utilisent des débits qui vont de 1 à 100 Mbit/s.
Nature du trafic	Analyse le trafic transitant sur la liaison.	Analyse tout le trafic transitant sur le réseau.
Sécurité	Nécessite l'ouverture de la liaison, l'introduction de l'analyseur peut être détectée.	L'analyseur peut être programmé pour ne pas répondre au broadcast, il est indécelable. Si les mots de passe ne sont pas cryptés, il peut les intercepter.

Figure 20.30 Comparaison des différents types d'analyseurs.

Un analyseur de protocoles de niveau N décode les données de service du niveau N (type de PDU, compteurs...) et fournit, en hexadécimal, le contenu du champ data, c'est-à-dire de la (N)SDU ou la (N + 1)PDU.

La trace proposée est une reproduction d'une trace obtenue avec un analyseur de protocole Ethernet. L'analyseur extrait le préambule, les fanions et ne présente que les données utiles. Le contenu de la trame en hexadécimal est interprété (codage ASCII), ce qui facilite le travail d'analyse.

En effet, le décodage du champ données laisse clairement apparaître son contenu : UNIX® System V... De ce fait, l'on sait déjà que l'on peut s'attendre à ce que le protocole réseau utilisé soit IP du DoD. La valeur des octets 13 et 14 (Ethertype ou type de protocole) confirment ces dires. Le protocole supérieur est TCP/IP (valeur 0x0800).

b) Méthode d'analyse

À partir de la structure du bloc de données rappelée dans l'énoncé. On découpe les données lues par l'analyseur en bloc de données à analyser (figure 20.31).

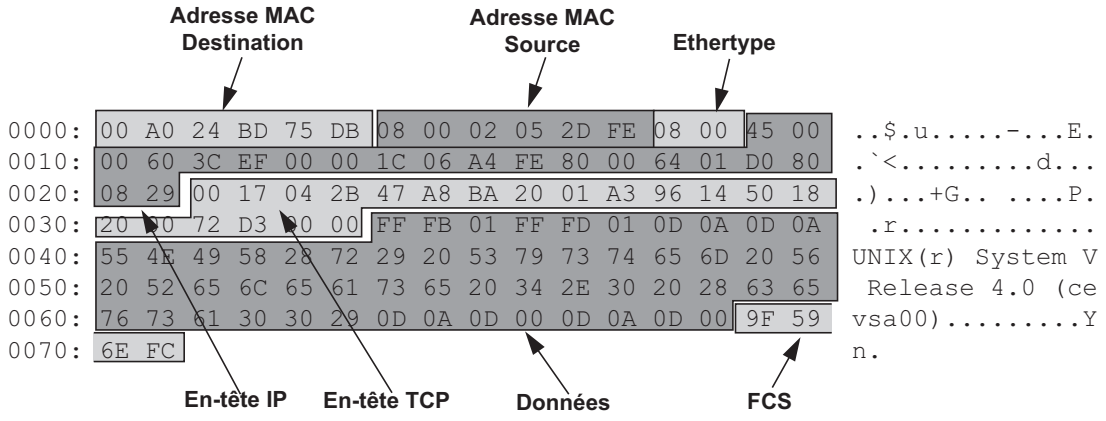


Figure 20.31 Découpage de la trame en bloc à interpréter.

Il ne reste plus alors qu'à interpréter champ par champ, octet par octet ou bit par bit, le résultat.

© Dunod – La photocopie non autorisée est un délit

Décodage trame MAC 1

1) En-tête MAC

Champ	Valeur hexa.	Commentaires
Adresse destination	00 A0 24 BD 75 BD	00 A0 24 Identification du fournisseur 3COM BD 75 BD N° séquentiel de fabrication de la carte
Adresse source	08 00 02 05 2D FE	08 00 02 Identification du fournisseur (ici 3 COM-Bridge)
Type de protocole	08 00	IP du DoD

2) En-tête IP

Champ	Valeur Hex.	Commentaires
Identification Version	4 -	Sur 4 bits, IP version 4
Longueur en-tête	- 5	IHL (*Internet Head Length*), sur 4 bits, en multiple de 4 octets la valeur normale est 5 soit 20 octets (pas d'option).
Type de service	00	Champ de bits Priorité (routine) – – – – – 0 0 0 Délai acheminement (Normal) – – – – 0 – – – Débit (Normal) – – – 0 – – – – Fiabilité (Normale) – – 0 – – – – – Réservés 0 0 – – – – – –
Longueur totale	00 60	Exprime la longueur totale du datagramme (données utiles de la couche MAC). Ici, la valeur 60 soit 96 octets est supérieure à 48, il n'y a donc pas eu d'opération de bourrage.
Identification	3C EF	Identifie tous les fragments d'un même datagramme.
Drapeau	00	Sur les trois derniers bits – bit 7, non utilisé – bit 6, DF (*Don't Fragment)*, à 0 : fragmentation possible – bit 5, MF (*More Fragment*), à 1 indique qu'un fragment suit. Les autres bits appartiennent au champ suivant.
Offset	00	Sur 13 bits, indique la position du fragment depuis le début.
Durée de vie	1C	*Time to Live*, durée de vie du fragment, initialement exprimé en seconde, représente aujourd'hui le nombre de bonds restants.
Protocole supérieur	06	Identifie TCP
Total de contrôle	A4 FE	
@ IP Source	80 00 64 01	@IP = 128.0.100.1, Adresse de classe B.
@ IP Destination	DO 80 08 29	@IP = 208.128.8.41, Adresse de classe C. En principe, les machines sur un même réseau appartiennent à un même espace d'adressage. Ce n'est pas le cas ici. On peut donc penser que la machine source n'est pas sur le même réseau physique que la station destinataire du message.

3) En-tête TCP

Champ	Valeur Hex.	Commentaires
Port source	00 17	Cette valeur identifie le terminal TELNET, le contenu des traces est donc un dialogue TELNET.
Port destinataire	04 2B	Attribué lors de l'établissement de la connexion.
N° de séquence	47 A8 BA 20	Le numéro de séquence initial est défini à la connexion, il est ensuite incrémenté du nombre d'octets transmis.
N° de seq. acquitté	01 A3 96 14	N° du prochain octet attendu (N° de séquence).
Longueur En-tête	50	Sur 4 bits, en multiple de 4 octets. L'en-tête TCP fait 20 octets (il n'y a pas d'option).
Drapeau	18	Champ de bits (6 bits valides) Fin (pas de demande de déconnexion) – – – – – – 0 Syn (utilisé seulement à la connexion) – – – – – – 0 – RST (pas de demande de réinit.) – – – – 0 – – PSH (délivrance immédiate) – – – – 1 – – – – – – 1 – – – – URG (pas de données urgentes) – – 0 – – – – –
Fenêtre	20 00	Fenêtre en réception de 8 192 octets (dynamique).
Total de contrôle	72 D3	Calculé sur l'ensemble du segment et pseudo en-tête IP.
Pointeur data URG	00 00	Pointeur sur données urgentes, non validé par le flag URG.

4) Champ données de TCP

```
                        FF FB 01 FF FD 01 0D 0A 0D 0A   .r..............
0040: 55 4E 49 58 28 72 29 20 53 79 73 74 65 6D 20 56  UNIX(r) System V
0050: 20 52 65 6C 65 61 73 65 20 34 2E 30 20 28 63 65   Release 4.0 (ce
0060: 76 73 61 30 30 29 0D 0A 0D 00 0D 0A 0D 00         sa00)........
```

Le champ données, reproduit ici, est partiellement décodé par l'analyseur (caractères interprétables). Cependant, l'analyse des premiers caractères du champ présente un intérêt certain :

'FF FB 01' et 'FF FD 01' sont des commandes TELNET (négociation d'options)

Toutes les commandes Telnet débutent par 'FF' (IAC, *Interpret As Command*, interpréter l'octet suivant comme une commande), si ce caractère apparaît dans le champ données il est doublé (caractère de transparence).

Le caractère suivant identifie la commande, il est éventuellement suivi d'un caractère qui précise une commande optionnelle. Les tableaux des figures 20.32 et 20.33 fournissent la liste des principales commandes et des options Telnet.

Dialogue Telnet, paramétrage de l'écho :

– 'FF FB 01' IAC WILL ECHO, Will Use Echo Data

– 'FF FD 01' IAC DO ECHO, Start Use Echo Data

© Dunod – La photocopie non autorisée est un délit

Commande	Valeur dec.	Valeur Hex.	Signification
IAC	255	FF	Interpréter le caractère suivant comme une commande
DON'T *xx*	254	FE	Refus d'une option, le caractère suivant '*xx*' identifie l'option refusée
DO *xx*	253	FD	Acceptation de l'option '*xx*' (Start Use)
WON'T *xx*	252	FC	Acquittement négatif de l'option '*xx*'
WILL *xx*	251	FB	Acquittement positif de l'option '*xx*' (Will Use)
GA	249	F9	Continuer (Go Ahead)
EL	248	F8	Effacer une ligne (Erase Line)
EC	247	F7	Effacer un caractère (Erase Character)
AO	245	F5	Arrêter l'édition (Abort Ouput)
IP	244	F4	Interrompre le processus (Interrupt Process)
BRK	243	F3	Break
NOP	241	F1	Opération nulle (Non OPeration)
EOR	239	EF	Fin d'enregistrement (End of Record)

Figure 20.32 Exemples de commandes Telnet.

Nom	Valeur dec.	Valeur Hex.	Signification
Transmit Binaire	00	OO	Transmission en mode 8 bits
Echo	01	01	Écho des données introduites au clavier (Echo Data)
Carriage Return	10	0A	Retour chariot, Positionne le curseur en début de ligne
Line Feed	13	10	Passage à la ligne suivante

Figure 20.33 Exemples d'options Telnet.

5) Champ FCS de la trame MAC

Valeur du FCS : 9F 59 6E FC.

Décodage Trame MAC 2 (figure 20.34)

L'analyseur précise que la longueur de la trame MAC est de 64 octets (figure 20.34), c'est-à-dire la longueur minimale d'une trame MAC Ethernet. Lorsque les données à transmettre ont une longueur inférieure à 64 octets, la couche MAC procède à un bourrage pour ramener la longueur du champ données MAC à 46 octets (64 octets en-tête MAC et FCS compris). Si on examine le champ longueur du datagramme IP (figure 12.29) on constate qu'effectivement la longueur du datagramme est de 0x29 (41 octets), il y a donc 5 octets de bourrage, ces 5 octets sont quelconques, c'est le contenu du buffer.

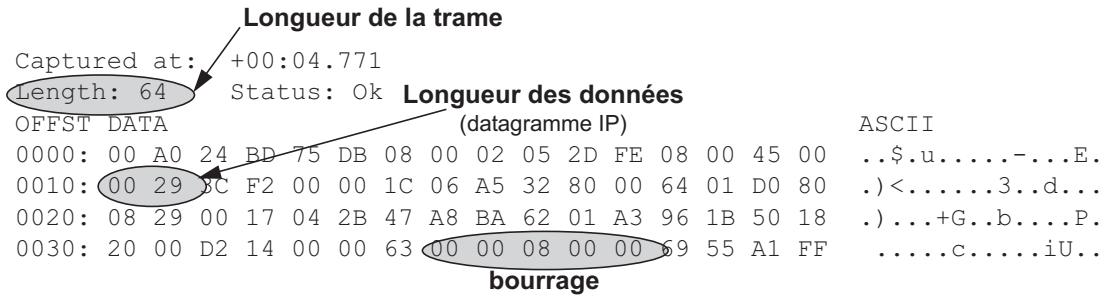


Figure 20.34 Trame MAC numéro 2.

CHAPITRE 11

11.1 SDH/PDH

Les principaux avantages s'expriment en termes de facilités d'exploitation, de fiabilisation des liaisons (autocicatrisation), de débit et de facilité à insérer ou à extraire un débit inférieur d'un lien.

11.2 Reconstitution d'un paquet d'appel

Pour reconstituer le paquet d'appel il faut d'abord coder tous les éléments le constituant :

1) Codage de l'adresse

Au format X.121, l'adresse Transpac est codé : Type d'accès, Département, Commutateur de rattachement, Numéro de la liaison. L'accès se faisant sur une LS, le type d'accès identifié par la valeur 1. Avec un chiffre par quartet, l'adresse de l'appelé est

```
1 75 01 0089
```

L'adresse est codée en DCB, premier chiffre dans le quartet de poids fort du premier octet du champ adresse.

2) Codage des facilités

- Facturation à l'appelé : 01, 01 ;
- GFA valeur locale 3 : 03,03 ;
- Taille paquet : $64 = 2^6,\ 128 = 2^7$ soit 42,06,07 ;
- Négociation taille fenêtre 2, 7 : 43,02,07 ;

Dans ces conditions, la longueur du champ facilité est 10 soit 0x0A.

Détermination du CV : pour un appel sortant, le NVL affecté à la voie logique est le NVL de plus grande valeur disponible. Ici, il s'agit de la première connexion soit 19 ou, en hexadécimal, 13.

© Dunod – La photocopie non autorisée est un délit

3) Format du paquet d'appel (figure 20.35)

Paquet	Binaire	Hexadécimal
GFI	0001 0000	10
NVL	0001 0011	13
Type paquet	0000 1011	0B
L. appelant / **L. Appelé**	0000 / 1001	09
Adresse appelé	0001 0111	17
	0101 0000	50
	0001 0000	10
	0000 1000	08
0 0 0 0	1001 0000	90
Longueur champ facilités	0000 1010	0A
Facturation à l'appelé	0000 0001	01
Oui	0000 0001	01
GFA	0000 0011	03
3	0000 0011	03
Taille paquet	0100 0010	42
Émission	0000 0110	06
Réception	0000 0111	07
Taille fenêtre	0100 0011	43
Émission	0000 0010	02
Réception	0000 0111	07

Figure 20.35 Codage d'un paquet d'appel.

11.3 Dialogue X.25

Rappels

La trace de niveau physique représente, codés en hexadécimal, tous les octets circulant sur la liaison. Avant d'entreprendre le décodage de ces valeurs, rappelons la structure générale de la trame LAP-B émise sur le niveau physique (figure 20.36) :

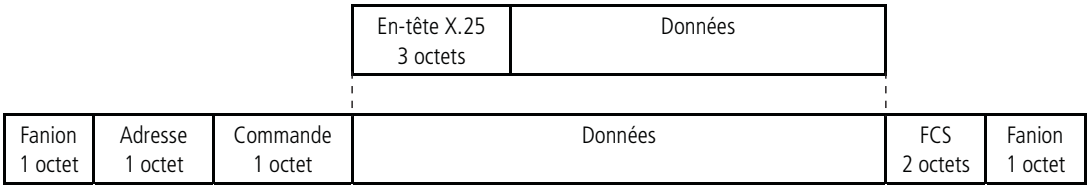


Figure 20.36 Trame LAP-B et paquet X.25

Examen de la trace ligne par ligne :

Ligne 1 à 3 ETCD 7E 01 0F 68 B9 7E

Hex	Binaire	Commentaires
7E	0111 1110	Fanion de début de trame, caractérisé par 6 uns consécutifs. Cette combinaison binaire ne devant pas se retrouver dans le champ d'information, tous les 5 bits à 1, un zéro est inséré, il est retiré à la réception (transparence binaire de la trame HDLC). Les fanions ne seront plus analysés dans la suite du décodage.
01	0000 0001	Champ adresse, valeur @1
0F	0000 1111	Trame de DM (***Disconnect Mode***), cette trame est émise par le réseau lors de la détection d'une rupture du lien physique. DM est répétée tous les T1. La rupture de la liaison est due à l'insertion de l'analyseur dans le circuit.
68		FCS
B9		FCS, les octets de FCS ne seront plus précisés dans la suite du décodage.
7E	0111 1110	Fanion de fin, ignoré dans la suite.

Ligne 4 ETTD 7E 01 3F EB 7F 7E

Hex	Binaire	Commentaires
01	0000 0001	Adresse, @1
3F	0011 1111	L'ETTD à la réception d'un état de déconnexion tente le rétablissement de la liaison en émettant la trame (U) ***SABM***.

Ligne 5 ETCD 7E 01 73 83 5E 7E

Hex	Binaire	Commentaires
01	0000 0001	Adresse, @1
73	0111 0011	ETCD acquitte cette trame par la trame (U) ***UA***, la liaison est rétablie.

Ligne 6 ETCD 7E 03 00 10 00 FB 07 A4 EA 6F 7E

Hex	Binaire	Commentaires
03	0000 0011	Adresse, @1
00	0000 0000	***Trame d'information***, P/F = 0, Ns = 0, Nr = 0
10	0001 0000 GFI GVL	Le champ d'information contient le paquet X.25-3, le premier quartet correspond au GFI, la valeur 0001 correspond à une utilisation du format normal (numérotation modulo 8). La N° de groupe de VL est le 0. Cet octet, identique dans le reste de la trace, ne sera plus commenté.
00	0000 0000	Les 8 bits suivants correspondent au Numéro de Voie Logique, soit le NVL 0. Rappelons que ce NVL est utilisé à des fins de servitude, sauf convention contraire à l'abonnement.
FB	1111 1011	Le troisième octet, indique le type de paquet, FB correspond à un paquet de ***demande de reprise***. En effet, la rupture du lien est considérée comme un incident grave, il est nécessaire de rétablir un état propre. Tous les circuits virtuels précédemment établis et maintenus par le réseau vont être détruits, les compteurs Ps et Pr sont réinitialisés à zéro. Le paquet de demande de reprise a été émis sur la VL 0, ce qui est conforme aux spécifications d'X.25.
07	0000 0111	Cet octet précise la cause de la demande de reprise, 7 correspond à une fin d'incident sur le réseau.
A4	1010 0100	Le diagnostic A4 indiqué signifie que l'incident a été détecté suite à une non-réponse à N2 (compteur de retransmission).

Ligne 7 ETTD 7E 03 21 A4 56 7E

Hex	Binaire	Commentaires
03	0000 0011	Adresse, @3
21	0010 0001	Cette trame est une trame de supervision ***RR***, elle acquitte la trame précédente, Nr = 1 (Compteur Nr, les trois bits de poids fort).

© Dunod – La photocopie non autorisée est un délit

Ligne 8 ETTD 7E 01 20 10 00 FF 8D 06 7E

Hex	Binaire	Commentaires
01	0000 0001	Adresse, @1
20	0010 0000	Il s'agit d'une ***trame d'information*** (premier bit à zéro), les compteurs valent Ns = 0 (première trame d'information émise), Nr = 1 (1 trame reçue).
10	0001 0000	GFI et Groupe de voies logiques.
00	0000 0000	NVL = 0
FF	1111 1111	Ce paquet est le paquet de ***confirmation de reprise***. La reprise étant acceptée par l'ETTD.

Ligne 9 ETCD 7E 01 21 14 98 7E

Hex	Binaire	Commentaires
01	0000 0001	Adresse, @1
21	0010 0001	Trame de supervision ***RR***, Nr = 1.

Ligne 10 ETTD 7E 01 22 10 03 0B 09 19 20 20 59 30 02 01 01 C4 01 00 67 89 7E

Hex	Binaire	Commentaires
01	0000 0001	Adresse, @1
22	0010 0010	***Trame d'information*** (I), Nr = 1, Ns = 1.
10	0001 0000	GFI et numéro de groupe de VL.
03	0000 0011	Le paquet a été émis sur le CV 3. Le paquet est sortant.
0B	0000 1011	Il s'agit d'un ***paquet d'appel sortant***. Les données relatives à cet appel suivent.
09	0000 1001	Longueur adresse appelant = 0 ; longueur adresse appelé : 9 quartets.
19	0001 1001	L'adresse est codée en DCB avec un chiffre par quartet, de ce fait :
20	0010 0000	L'adresse est directement lue, il s'agit de :
20	0010 0000	1 92 02 0593
59	0101 1001	
30	0011 0000	Le dernier quartet est un quartet de bourrage.
02	0000 0010	Longueur du champ facilités
01	0000 0001	Facilité de taxation au demandé ou (et) sélection rapide suivant la position des bits de l'octet suivant.
01	0000 0001	Taxation au demandé.
C4	1100 0100	Données utilisateur
01	0000 0001	idem.
00	0000 0000	idem.

Ligne 11 ETCD 7E 01 41 12 14 7E

Hex	Binaire	Commentaires
01	0000 0001	Adresse, @1
41	0100 0001	Trame de supervision ***RR***, Nr = 2.

Ligne 12 ETCD 7E 03 42 10 03 0F 70 A9 7E

Hex	Binaire	Commentaires
03	0000 0011	Adresse, @3
42	0100 0010	***Trame d'information***, Ns = 1, Nr = 2.
10	0001 0000	GFI ...
03	0000 0011	NVL = 3
0F	0000 1111	***Paquet d'acceptation d'appel***, le paquet d'appel a été accepté par l'ETTD distant, le niveau 3 est établi.

Ligne 13	**ETTD**	**7E**	**03**	**41**	**A2**	**DA**	**7E**

Hex	**Binaire**	**Commentaires**
03	0000 0011	Adresse, @3
41	0100 0001	Trame de supervision ***RR***, Nr = 2

Ligne 14	**ETTD**	**7E**	**01**	**44**	**10**	**03**	**00**	**E0**	**00**	**00**	**01**	**00**	**20**	**08**	**00**	**10**	**00**
		C2	**00**	**50**	**49**	**00**	**08**	**08**	**00**	**00**	**00**	**50**	**52**	**00**	**08**	**00**	**00**
		0E	**60**	**50**	**6B**	**00**	**14**	**02**	**00**	**00**	**23**	**01**	**00**	**10**	**01**	**18**	**50**
		C9	**05**	**00**	**00**	**00**	**00**	**01**	**24**	**7E**							

Hex	**Binaire**	**Commentaires**
01	0000 0001	Adresse, @1
44	0100 0100	***Trame d'information***, Ns = 2, Nr = 2.
10	0001 0000	GFI ...
03	0000 0011	NVL = 3.
00	0000 0000	Type de paquet, ***paquet de données*** Ps = 0, Pr = 0.
E0	1110 0000	Champ de données, il correspond à un rétablissement de la connexion de transport en environnement propriétaire DSA (BULL).

Le schéma de la figure 20.37 représente le diagramme des échanges.

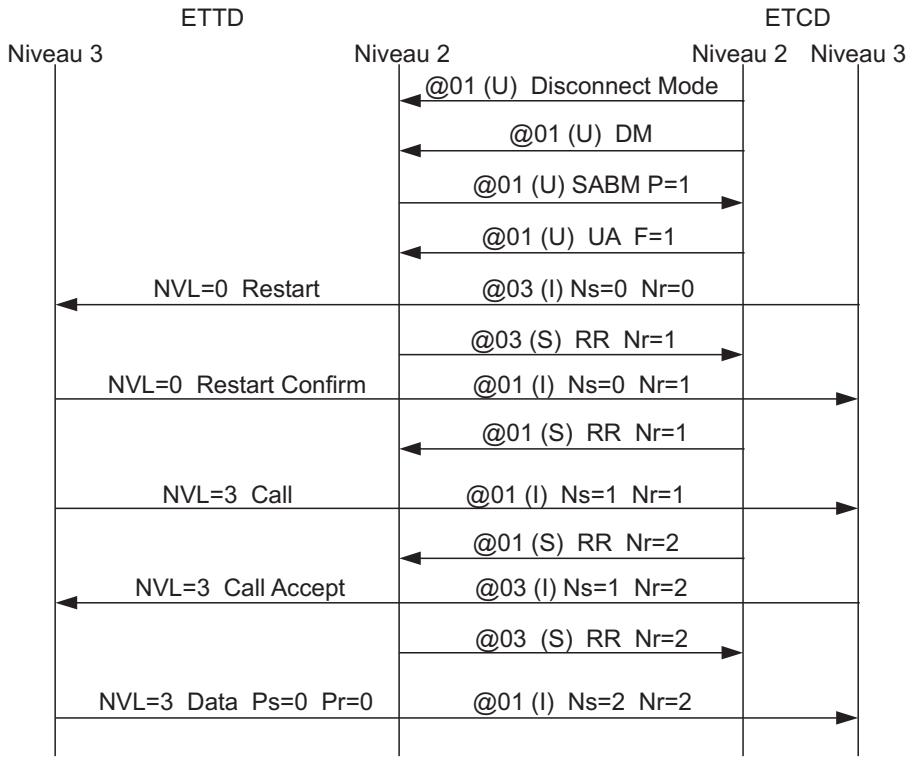


Figure 20.37 Dialogue ETTD/ETCD suite à une rupture du lien physique.

© Dunod – La photocopie non autorisée est un délit

11.4 Définition d'un protocole

a) Valeur optimale de la taille de l'unité de données.

Cette valeur correspond au minimum de la fonction $T(p)$. Il convient donc de rechercher la valeur de p qui annule la dérivée première :

$$Tp = \frac{L + pH}{D}\left(1 + \frac{N}{p}\right) = \frac{L}{D} + \frac{LN}{Dp} + \frac{pH}{D} + \frac{HN}{D}$$

$$T'(p) = -\frac{LN}{D\,p^2} + \frac{H}{D}$$

La valeur qui annule cette fonction est :

$$p = \sqrt{\frac{LN}{H}}$$

soit

$$p = \sqrt{\frac{1\,500 \times 3{,}25}{5}} = 31{,}225 \text{ paquets (seule la solution positive est retenue !).}$$

L'étude des variations de la fonction ou du signe de la dérivée seconde montre qu'il s'agit bien d'un minimum. Ce qui correspond à une longueur de paquets de

$$Lp = \frac{1\,500}{31{,}225} = 48 \text{ octets.}$$

b) Contrôle de flux

Pour déterminer l'efficacité de contrôle de flux, il convient de définir l'inertie du système. C'est-à-dire combien de paquets seront envoyés entre le paquet saturant et la réception par la source du message de demande d'arrêt.

Si on tient compte que du temps de transfert sur le réseau, cette valeur correspond au nombre de paquets (W) émis pendant le trajet aller et retour d'un message (Ta) soit $W = Ta/tb$ où tb correspond au temps d'émission d'un paquet

1) En interne au réseau

$Ta = 2 \cdot 10^5/2 \cdot 10^8 = 1$ ms

$tb = (53.8)/622 \cdot 10^6 = 0{,}68 \cdot 10^{-6}$ s

$W = 10^3/0{,}68 \cdot 10^{-6} = 1\,470$

Soit 1 470 paquets de 53 octets qui auront été émis inutilement. Ce mode de contrôle de flux est inefficace (temps de réaction) sans compter que ces paquets devront être mémorisés pour être retransmis !

2) À l'interface usager

$Ta = 4 \cdot 10^4/2 \cdot 10^8 = 2 \cdot 10^{-4}$

$tb = (53.8)/2{,}048 \cdot 10^6 = 0{,}207 \cdot 10^{-3}$

$W < 1$

Dans ce cas, le contrôle de flux peut être très efficace, l'émission est arrêtée immédiatement.

Dans ce réseau on pourrait donc envisager un contrôle de flux à l'interface usager/réseau, et aucun contrôle en interne au réseau.

c) Nombre de connexions simultanées (nombre de CV)

Si n en bits est la capacité de numérotation des CV, le nombre de CV est 2^n, dans notre cas $N = 2^{28} = 286\,435\,456$.

d) Taux d'erreur dans le réseau

1) Probabilité qu'un paquet transite sans erreur sur 1 lien

Si Teb est la probabilité qu'un bit soit erroné, la probabilité qu'un bit ne le soit pas est de $1 - \text{Teb}$

et pour un bloc de N bits,

$$\text{P}_\text{a} = (1 - \text{Teb})^N$$

Avec $\text{Teb} = 10^{-9}$,

$$N = 53 \times\ 8 = 424 \text{ bits}$$

2) Pour l'ensemble des 3,25 nœuds soit 4,25 liens traversés par un paquet

$$\text{P}_\text{b} = \text{Pa}^9 = (1 - \text{Teb})^{4{,}25N} = (1 - 0{,}000000001)^{1\,802} = 0{,}999998198$$

c) Taux d'erreur pour l'ensemble du réseau

$$\text{Teb}' = 1 - 0{,}999998198 = 0{,}000001801 \quad \text{soit} \quad 1{,}8 \cdot 10^{-5}$$

e) Temps de traversée du réseau et gigue

Non, il n'est pas possible de borner le temps de transit dans le réseau. Le temps minimal correspond au cas où aucune erreur ne se produirait (Tmin), dans tous les autres cas, le temps dépend du nombre de reprises sur erreur réalisées dans le réseau, la gigue ne peut donc être estimée.

f) Modem d'accès distant

1) Débit maximal envisageable sur le lien

$$C = BP \log_2(1 + S/N) = 3\,100\ \log_2(1\,001) \approx 3\,100 \times 10 = 31\,000 \text{ bit/s}$$

2) Valence du signal

Le modem envisagé utilise une modulation de phase et d'amplitude à 16 états (MAQ16). Est-ce réalisable ? La valence maximale compte tenu du rapport signal à bruit est :

$$v = \sqrt{1 + \frac{S}{N}} = \sqrt{1001 = 31{,}6}$$

Rien ne s'oppose donc à l'utilisation d'une modulation MAQ16.

3) Débit du modem

$$D = 2BP \log_2 v = 2 \cdot (3\,400 - 300) \log_2 16 = 2 \cdot 3\,100 \times 4 = 24\,800 \text{ bit/s}$$

© Dunod – La photocopie non autorisée est un délit

11.5 Protocole ATM

Chaque commutateur ATM réalise la fonction d'adaptation des débits par l'insertion et l'extraction de cellules vides. Les cellules vides sont identifiées par une valeur spécifique de l'entête : 0x00-00-00-01 ou seul le bit CLP (priorité à l'écartement est positionné). L'utilisation de cellules vides interdit donc l'emploi de la liaison virtuelle de VPI/VCI 0/0.

11.6 Priorité ou réservation de ressources

Si l'implémentation des protocoles à niveaux de priorité est plus simple que celle des protocoles à réservation de ressource, ils nécessitent un surdimensionnement des réseaux or, si le réseau est largement surdimensionné la notion de priorité n'a plus d'utilité.

Cependant, aucune prévision sur les trafics soumis ne peut être réalisée, une surcharge du réseau peut toujours se produire et dans ces conditions tous les flux sont pénalisés y compris les flux prioritaires.

Enfin, si tous les flux sont prioritaires, la notion de priorité n'a aucune utilité.

Seuls, les systèmes à réservation de ressources sont susceptibles de satisfaire pleinement les exigences des flux isochrones. Cependant, ces systèmes nécessitent un système de signalisation beaucoup plus complexe et un trafic de gestion du réseau plus important.

11.7 Encapsulation de données

1) Débit théorique du système

a) Bande occupée par une tonalité 120 Hz (100 + 20).

b) Nombre de tonalités :
- Bande passante du système : 3 800 – 200 = 3 600 Hz ;
- Nombre de tonalités : 3 600/120 = 30 tonalités.

c) Débit maximum du système $30 \times 128 \times 8 = 30\,720$ bit/s.

2) Débit pratique du système

a) Puissance maximale reçue : lecture du tableau 9 mW.

b) Puissance minimale acceptée par le système, -3 dB correspond à une tonalité de demi-puissance soit 4,5 mW.

c) La lecture du tableau fait apparaître 25 tonalités $>$ 4,5 mW.

d) Débit effectif du modem $25 \times 128 \times 8 = 25\,600$ bit/s.

3) Rendement du système

a) Le nombre d'octets de bourrage varie de 0 à 47 octets.

b) Nombre de cellules ATM :
Taille des données AAL5 avant bourrage 1 500 + 8 = 1 508 octets
Nombre de cellules ATM 1 508/48 = 31,4 cellules soit 32 cellules entières.

c) Valeur des différents champs (figure 20.38) :
- Taille des données AAL5 après bourrage : $48 \times 32 = 1\,536$ octets ;
- Données de bourrage : $1\,536 - 1\,508 = 28$ octets.

Soit le schéma d'encapsulation suivant (figure 20.38) :

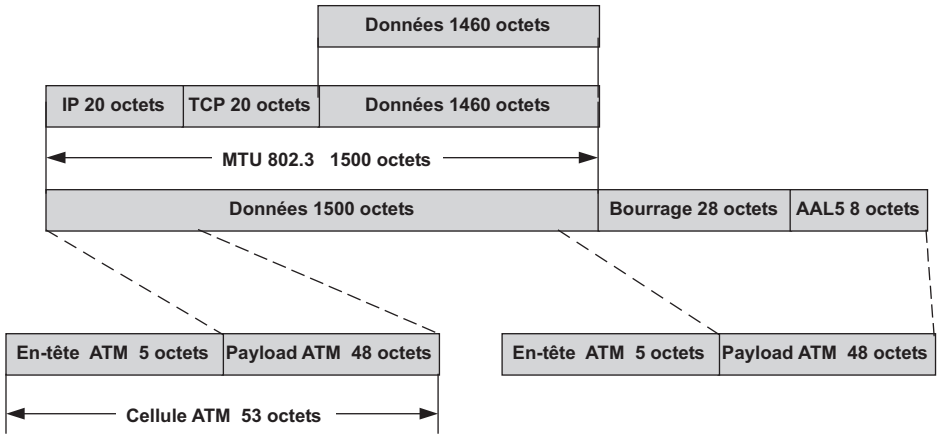


Figure 20.38 Encapsulation des données.

d) Rendement du protocole :
Données utiles 1 460 octets, données transmises $32 \cdot 53 = 1\,696$ octets
Rendement du protocole 1 460/1 696 = 86 %

e) Taux de transfert d'information :

$$\text{Débit réel du modem} \times \text{Rendement du protocole} = 25\,600 \times 0{,}86 = 22\,016 \text{ bit/s}$$

f) Taux de transfert d'information en tenant compte du taux d'erreur :

Probabilité de recevoir l'ensemble des informations non erronées (p) :

$$p = (1 - 0{,}000001)^{1\,696 \cdot 8} = 0,987$$

$$\text{TTI} = 22\,016 \times 0{,}987 = 21\,730 \text{ bit/s.}$$

g) Rendement global du système :

$$R = \text{TTI}/\text{Débit potentiel du modem} = 21\,730/30\,720 = 0{,}707 \text{ soit environ } 71\ \%.$$

11.8 Évolution de l'encapsulation d'IP

Type d'encapsulation	Mise en œuvre	Caractéristiques
IP/ATM/SDH/WDM	Solution actuelle la plus utilisée par les opérateurs pour transporter IP.	L'avantage essentiel est l'utilisation de l'existant. Le flux IP peut bénéficier de la qualité de service d'ATM (transport de la voix et de la vidéo).
IP/SDH/WDM	Utilisation directe des boucles SDH existantes	Gain d'« overhead », mais IP directement sur une couche de multiplexage n'assure pas l'utilisation optimale de la bande passante.
IP/WDM	Réalisation de réseau intégralement IP par liaison optique directement entre les routeurs IP.	Permet de garantir l'homogénéité du traitement de la qualité de service (IP de bout en bout). L'optimisation de la bande passante peut être obtenue par l'utilisation de MPLS (G-MPLS)

Figure 20.39 Encapsulation IP.

© Dunod – La photocopie non autorisée est un délit

CHAPITRE 12

12.1 Distinction entre CSMA/CD IEEE 802.3 et Ethernet.

La figure 20.40 rappelle le format de la trame IEEE 802.3. Ethernet et 802.3 se distinguent par l'octet « longueur des données ». Le champ longueur des données exprime, en 802.3, la longueur des données utiles de la trame MAC. En Ethernet ce champ identifie le protocole de niveau supérieur, charge à ce dernier de distinguer les données utiles d'éventuelles données de bourrage.

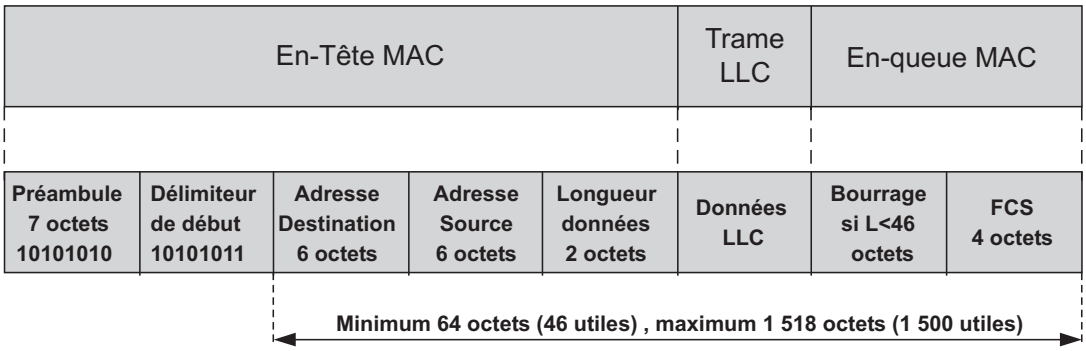

En-Tête MAC
Trame LLC
En-queue MAC
Préambule 7 octets 10101010
Délimiteur de début 10101011
Adresse Destination 6 octets
Adresse Source 6 octets
Longueur données 2 octets
Données LLC
Bourrage si L<46 octets
FCS 4 octets
Minimum 64 octets (46 utiles) , maximum 1 518 octets (1 500 utiles)

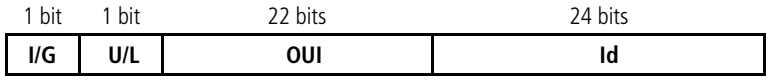
Figure 20.40 Rappel du format de la trame IEEE 802.3.

La longueur des données utiles est, au maximum, de 1 500 octets (0x05DC). Toute valeur de ce champ supérieure à 1 500 identifie un protocole et non une longueur de données. Par exemple, La valeur 2 048 (0x0800) identifie le protocole IP de la pile TCP/IP.

12.2 Adressage MAC

a) Le format de l'adresse MAC

Voir figure ci-dessous (figure 20.41) :



I/G : I = 0 adresse unicast
G = 1 adresse de diffusion
U/L : U = 0 adresse universelle
L = 1 adresse locale (fixée par l'administrateur)
OUI : Identifiant du constructeur de l'interface réseau (NIC)
Id : Identifiant séquentiel attribué par le constructeur

Figure 20.41 Adressage MAC.

b) Adresses de réponse

Un coupleur réseau doit pouvoir répondre aux adresses unicast, multicast, broadcast.

c) Type d'adresse

Sachant que pour l'IEEE, les bits de poids faible sont émis devant (numérotation des bits de 0 à 31 de gauche à droite, format canonique), l'adresse 01-00-5E-AB-CD-EF est une adresse de type multicast. Le premier octet 0x01, noté selon l'IEEE, donne en binaire 10000000. Il s'agit donc bien d'une adresse de diffusion.

d) Type d'application

L'application peut être de la diffusion vidéo.

12.3 Notation canonique et non canonique

Le format IEEE, dit canonique, correspond à l'écriture des octets bits de poids faible devant, le format non canonique à l'écriture naturelle. Ainsi, la valeur non canonique 1 vaut en écriture canonique 128. Passer de la forme canonique à la forme non canonique, ou l'inverse, correspond donc à inverser l'ordre des bits. Les écritures sont différenciées par les séparateurs, le tiret « - » pour la forme non canonique et 2 points « : » pour la forme canonique. Aussi, l'adresse de diffusion générale s'écrit :

FF-FF-FF-FF-FF-FF en format non canonique et

FF:FF:FF:FF:FF:FF en format canonique.

12.4 Comparaison des topologies et des méthodes d'accès

Le tableau de la figure 20.42 effectue une comparaison succincte des topologies, en ne retenant que les topologies de base : bus, étoile et anneau.

Topologie	Avantages	Inconvénients
Bus	Diffusion aisée de messages. Insertion de stations sans interrompre le trafic.	Collision de messages. Limitation des distances (atténuation)
Étoile	Diffusion aisée par le concentrateur. Conflit d'accès réglé par le concentrateur. Insertion de stations sans interrompre le trafic, mais nécessite généralement une reconfiguration du concentrateur.	Sensibilité à la défaillance du concentrateur. Nombre de stations limité par le nombre de ports disponibles. Performances liées à la puissance de calcul du nœud.
Anneau	Liaison point à point, ce qui facilite l'utilisation de la fibre optique. Régénération du signal par chaque station, ce qui augmente la portée du réseau.	Diffusion difficile. L'insertion de stations rompt l'anneau. Complexité du coupleur (retrait et insertion d'information).

Figure 20.42 Comparaison des topologies de base.

Le tableau de la figure 20.43 réalise une brève comparaison des principales méthodes d'accès.

© Dunod – La photocopie non autorisée est un délit

Méthode d'accès	Avantages	Inconvénients
CSMA/CD	Simplicité de l'algorithme. Excellente performance à faible charge	Les collisions pénalisent rapidement les performances dès que la charge augmente. Accès non équitable et non déterminé (accès probabiliste)
Jeton adressé	Accès déterministe et équitable. Mécanisme de priorité. Synchronisation des horloges (circulation permanente d'un message). Pas d'effondrement à forte charge.	Reconfiguration de l'anneau logique à chaque ajout ou retrait de station. Complexité de l'algorithme d'accès.
Jeton non adressé	Accès déterministe et équitable. Mécanisme de priorité.	Difficulté de gestion de l'anneau (station de surveillance). Insertion et retrait des données.

Figure 20.43 Comparaison des principaux algorithmes d'accès.

12.5 Séquence de synchronisation bit en 802.3 et 802.5

Un réseau 802.3 est caractérisé par l'asynchronisme des émissions, il peut y avoir de longs temps de silence entre deux messages. La dérive des horloges peut être importante (réseau plésiochrone), il est donc nécessaire d'avoir une longue séquence de resynchronisation.

En 802.5, même en l'absence de communication entre les stations, le jeton circule. Les stations sont donc périodiquement resynchronisées (réseau synchrone) ; la séquence de synchronisation peut être supprimée.

12.6 Rapidité de modulation

Le codage du signal dans un réseau 802.3 est en Manchester (Biphase), ce type de codage se caractérise par une transition au milieu de chaque temps bit, il y a donc deux états par temps bit ; la rapidité de modulation est le double du débit soit 20 Mbauds.

Autre explication : le codage Manchester correspond à un codage nB/mB. En effet, un 0 correspond à l'émission de 01 (niveau électrique) et un 1 correspond à l'émission de 10 (niveau électrique), la vitesse de signalisation sur la ligne ou rapidité de modulation est bien le double du débit binaire.

12.7 Longueur virtuelle de l'anneau 802.5

Insérer une station revient à allonger le temps de parcours d'un temps bit, donc à augmenter la longueur virtuelle de l'anneau de la taille d'un bit. La taille d'un bit (L) est donnée par :

$$L = \text{durée d'un bit} \times \text{vitesse de propagation} = t \times V$$

avec V vitesse de propagation égale à $V = v \times c$

v est le coefficient de vélocité du câble c est la vitesse de la lumière.

$$V = (2/3) \times 3 \cdot 10^8 = 2 \cdot 10^8 \text{ m/s} \Rightarrow 200 \text{ m/}\mu\text{s}$$

et

$$\text{t} = 1/\text{Débit} = 1/(4 \cdot 10^{-4}) = 0{,}25 \ \mu\text{s}$$

alors

$$\text{L} = 0{,}25 \times 200 = 50 \text{ m}$$

L'insertion d'une station accroît la longueur virtuelle de l'anneau de 50 m.

12.8 Conception d'un réseau Ethernet à 100 Mbit/s

Fenêtre de collision

Le fonctionnement du CSMA/CD repose sur la possibilité de détection des collisions par toute station qui émet. La fenêtre de collision correspond à deux fois la durée de propagation entre les deux stations les plus éloignées ce qui, ici, correspond à :

$$\text{Time Slot} = (2 \times 200)/200\,000 = 2 \text{ ms}$$

Le temps d'émission de la plus petite trame doit être d'au moins 2 ms.

Temps effectif d'émission

Temps d'émission d'une trame de 4 500 octets :

$$\text{T} = \text{Longueur Trame}/\text{Débit} = (4\,500 \times 8)/100 \cdot 10^6 = 0{,}36 \text{ ms}$$

Conclusion

Le protocole CSMA/CD ne peut convenir à cette réalisation. Le message minimum devrait avoir pour longueur :

Le time slot correspond au temps d'émission minimal de la station :

Longueur en bits = Time Slot × Débit

$\text{L} = 2 \cdot 10^{-3} \times 100 \cdot 10^6 = 200 \cdot 10^3$

$\text{L}_{\text{octets}} = 200\,000/8 = 25\,000$

soit une trame de 25 000 octets ce qui, compte tenu du fait que la plupart des messages sur un réseau local ont une longueur moyenne inférieure à 256 octets, conduit à des séquences de bourrage très importantes et par conséquent à une efficacité du protocole pratiquement nulle.

12.9 Efficacité du protocole 802.5 à 100 Mbit/s

Le débit du réseau réel peut être mesuré par le rapport entre la longueur en bits du message à émettre et le temps d'occupation du réseau (laps de temps avant l'émission suivante).

© Dunod – La photocopie non autorisée est un délit

Temps d'occupation du support

Temps d'occupation du support = T de transmission + T de rotation + T de retard :

Temps de transmission = (L × 8)/100· 10^6 = 0,36 ms ;

Temps de rotation = (Distance/v) = 200/200 000 = 1 ms ;

Temps de retard = retard une station × Nombre de stations ;

Temps de retard d'une station = 1 temps bit = 1/100 10^6 = 10^{-8} s.

Temps d'occupation (en ms) $= 0{,}36 + 1 + 10^{-5} = 0{,}36 + 1 + 0{,}01 = 1{,}37$ ms.

Efficacité du réseau

$$\text{Débit} = \text{Longueur du message}/\text{Temps d'occupation}$$
$$= (4\,500 \times 8)/1{,}37 \cdot 10^{-3} = 26{,}3 \text{ Mbit/s}.$$

L'efficacité de ce réseau n'est que d'environ 25 %.

Les réseaux à jeton à haut débit implémentent un protocole similaire au 802.5 mais autorisent plusieurs jetons sur le réseau, c'est le cas notamment du réseau Token Ring à 16 Mbit/s d'IBM, et du FDDI.

12.10 Temps de rotation du jeton

Le cas le plus défavorable correspond à l'attente active du jeton par une station (la station désire émettre) alors que le jeton est détenu par la station qui la suit dans l'anneau et que toutes les stations sont aussi en attente active et utilisent leurs temps de parole au maximum.

Temps d'occupation de l'anneau par chaque station

Temps d'émission + temps de rotation + retard apporté par les stations traversées

$$= 10 + 0{,}0125 + 0{,}0125 = 10{,}025 \text{ ms}$$

avec :

Temps d'émission = 10 ms ;

Temps de rotation = longueur de l'anneau/vitesse = (50 × 50)/200 = 12,5 µs ;

Temps de retard = Temps bit × NB stations = $(1/4 \cdot 10^{-6}) \times 50 = 0{,}25$ µs × 50 = 12,5 µs.

Pour les $N - 1$ stations du réseau qui vont émettre avant :

Temps d'attente du jeton $= 49 \times 10{,}025 = 491{,}225$ ms soit $\approx 1/2$ seconde.

Débit utile pour cette station

Efficacité = Temps d'émission/temps total = 10/491 = 0,02 soit 2 % ;

Le débit effectif pour cette station est de : 4 Mbit × 0,02 = 80 000 bit/s.

Réseaux CSMA/CD

Ce calcul n'est pas réalisable pour un réseau Ethernet, on ne peut que calculer la probabilité d'accès au média pendant un intervalle de temps. Le CSMA/CD est dit probabiliste alors que le 802.5 est dit déterministe puisque l'on peut déterminer une borne maximum au droit à parole.

12.11 Commutateur ou hub ?

Lorsqu'un réseau est peu chargé, la probabilité de collision est faible, le hub diffuse les trames sans stockage ni analyse, il est par conséquent plus efficace qu'un commutateur. Dès que la charge du réseau augmente, les commutateurs sont alors plus performants.

Objectifs	Equipement recommandé
Réseaux données peu chargés, recherche de la performance	hub
Réseaux données très chargés, recherche de la performance	commutateur
Réseaux voix/données sur IP	commutateur

Figure 20.44 Equipement et objectifs.

Pour des services de type voix, il faut garantir le temps de transfert, indépendamment de la charge du réseau, seuls alors, les commutateurs répondent au problème. En pratique, un réseau de hub, faiblement chargé, peut être suffisant.

12.12 Plan d'adressage d'une entreprise

Ce problème a plusieurs solutions, celle exposée n'en est qu'une parmi d'autres.

Adressage du réseau

L'adresse privée 10.0.0.0 est une adresse de classe A, c'est-à-dire qu'elle comporte un octet d'identification du réseau (Net_ID) et 3 octets pour numéroter les stations (Host_ID).

On doit pouvoir distinguer les sites et dans chaque site 10 sous-réseaux. Une solution simple consiste à réserver le second octet à l'identification des établissements en adoptant le numéro de département. Le troisième octet peut alors être utilisé pour numéroter les sous-réseaux, le quartet de poids fort étant suffisant (2^4). Dans ces conditions, l'adresse réseau est 10.0.0.0 et le masque de sous-réseau 255.255.240.0.

L'adressage des liaisons

Deux techniques peuvent être utilisées pour adresser les liaisons : soit considérer chaque LL comme un réseau (adressage point à point), soit considérer l'ensemble des LL du réseau comme appartenant au même réseau. La première technique, plus simple, sera utilisée ici. L'adressage des LL peut être quelconque, ces adresses ne sont utilisées que par les routeurs pour choisir le port de sortie (identification d'un port), dans ces conditions elles ne sont jamais vues de l'extérieur. La figure 20.45 ci-dessous illustre l'une des solutions possibles.

Pour identifier les liaisons nous avons adopté une numérotation significative de classe A :

– le premier octet 80 indique le réseau de LL ;

– le second qu'il s'agit du réseau 10 ;

– les troisième et quatrième octets identifient les extrémités.

© Dunod – La photocopie non autorisée est un délit

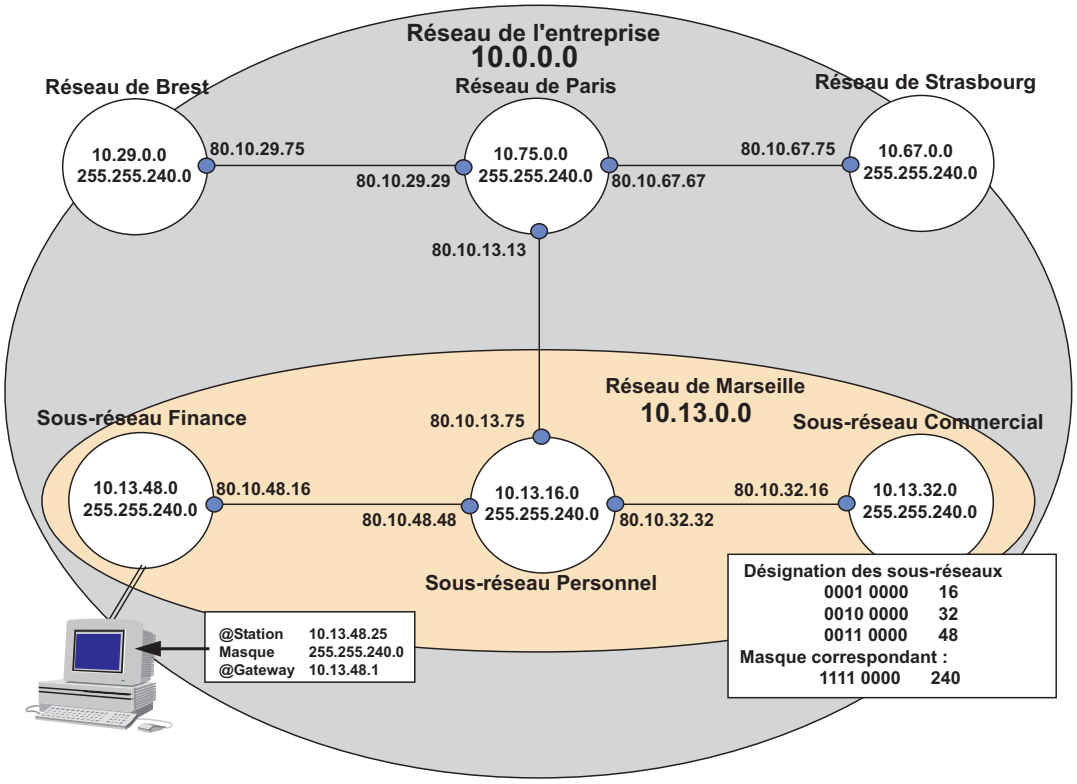


Figure 20.45 Illustration d'une solution envisageable.

CHAPITRE 13

13.1 FDDI et Token Ring

	Token Ring	FDDI
Débit	4 ou 16 Mbit/s	100 Mbit/s
Technique d'accès	Jeton non adressé et technique de l'ERT (version 16 Mbit/s)	Jeton non adressé, temporisé et technique de l'ERT
Codage	Manchester différentiel	4B/5B et NRZI
Unité de données	4 500 octets (4 Mbit/s) 18 000 octets (16 Mbit/s)	4 500 octets
Priorité	8 niveaux	8 niveaux
Topologie	Simple anneau (version IBM, double anneau)	Double anneau
Distance	300 m entre stations Portée quelques km	2 km entre stations 100 km

Figure 20.46 Comparaison FDDI/Token Ring.

13.2 Données de la classe Isochrone

Traditionnellement, le transport de la voix nécessite de garantir la délivrance des échantillons (valeur) à un rythme précis, soit un échantillon toutes les 125 μs. Ceci nécessiterait dans FDDI-1 que le TTRT (*Target Token Rotation Time*) soit de 125 μs. Ce qui compte tenu du diamètre envisageable pour le réseau est inconcevable (100 km à $2 \cdot 10^8$ m/s correspond à un temps de 0,5 ms). C'est pour cette raison que les réseaux FDDI-2 et DQDB ont organisé le transfert de données à partir de trames dont la fréquence de récurrence est de 8 000 Hz (période de 125 μs).

Cependant, la technique du jeton temporisé est tout à fait à même d'assurer un transfert de la voix en mode paquets, les contraintes temporelles étant alors moins strictes. Un paquet voix de 20 octets requiert un TTRT de 2,5 ms (20×125 μs).

13.3 L'acquittement dans FDDI

Rappelons que dans FDDI le champ de statut de trame (**FS**) comporte les indications d'erreur, d'adresse reconnue et de trame recopiée. Il contient au moins trois symboles respectivement désignés E (erreur détectée), A (adresse reconnue) et C (trame recopiée). Chacun de ces symboles est mis au 0 logique par l'émetteur de la trame (symbole R) ; la station qui détecte une erreur positionne le champ E au 1 logique (symbole S). De même, chaque station qui reconnaît son adresse positionne le champ A à 1 logique (symbole S) et, si elle recopie correctement la trame, le champ C à 1 logique (symbole S) ; sinon ce champ reste à 0 logique (symbole R).

	E	A	C	A	C	A	C
État	Reset	Set	Set	Set	Set	Set	Reset
Binaire	00111	11001	11001	11001	11001	11001	00111

Figure 20.47 Composition du champ FS.

Dans la figure 20.47, le champ FS indique qu'aucune station de l'anneau n'a détecté une erreur (Champ E = Reset), trois stations ont reconnu leur adresse (3 champs « A » à Set), mais seulement deux ont correctement recopié la trame (2 champs « C » à Set, un à Reset).

13.4 Rotation des données sur le réseau FDDI

La circulation des données est illustrée figure 20.48. Dans le schéma 1, la station A a acquis le jeton et émet sa trame, en 2, après l'émission de sa trame elle génère un jeton sur le réseau. En 3, C reconnaît son adresse, il recopie la trame. Pendant ce temps, en 4, B acquiert le jeton et émet ses données. À l'instar de A, à la fin de son émission, il insère un jeton. En 5, A reçoit les données qu'il a émises, il les retire de l'anneau. Il n'a pas besoin de régénérer un jeton puisqu'il l'a déjà fait après son émission de données (**ETR**, *Early Token Release*). En 6, D a reconnu son adresse, il recopie les données. Il n'y a plus que les données de B sur le réseau que ce dernier retirera lorsqu'elles lui arriveront.

© Dunod – La photocopie non autorisée est un délit

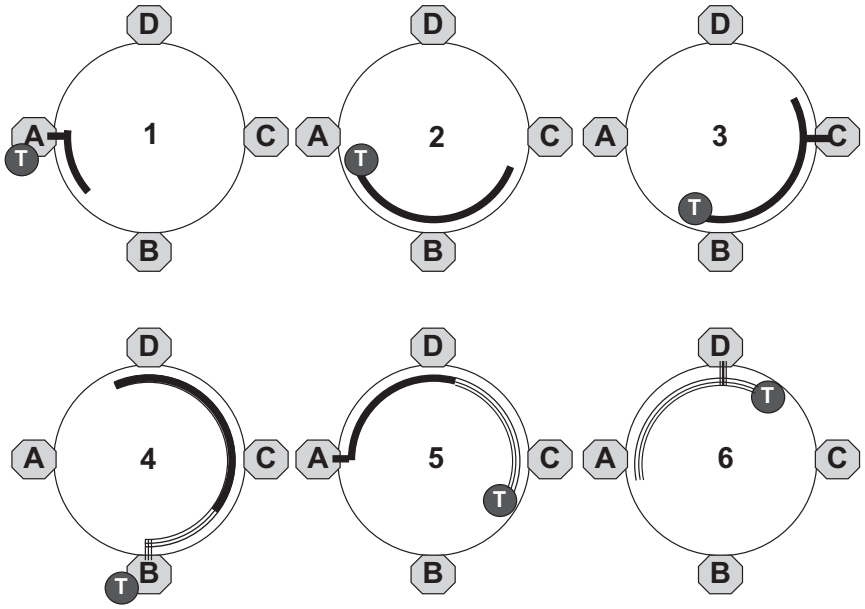


Figure 20.48 Circulation des données dans le réseau FDDI.

13.5 État des compteurs dans DQDB

Le compteur **RQ** (*Request Counter*) compte les requêtes formulées par les stations amont, à 5 il indique que 5 stations ont formulé une demande d'émission. Le compteur **CD** (*Count Down*) est décrémenté à chaque fois qu'une cellule vide est identifiée par la station, 2 slots vides ont donc déjà été reconnus.

La station devra encore décompter 3 slots vides pour satisfaire les demandes amont. Elle déposera ses données dans le quatrième slot vide décompté à partir de l'état décrit dans l'exercice.

CHAPITRE 14

14.1 Interconnexion d'un réseau 802.3 et 802.5

L'approche fondamentalement différente des deux réseaux impose une conversion de protocole de niveau MAC. Les différents problèmes à résoudre sont :

a) Passage du réseau 802.3 (Ethernet) au réseau 802.5 (Token Ring) :

- reformatage des trames,
- inversion de l'ordre des bits,
- gestion d'une priorité fictive,
- recalcul du FCS,
- le pont devra assurer la purge de l'anneau,
- les buffers devront être suffisamment dimensionnés si le 802.5 n'est qu'à 4 Mbit/s (congestion).

b) Passage du réseau 802.5 (Token Ring) au réseau 802.3 (Ethernet) :

- reformatage des trames en générant éventuellement du bourrage,
- inversion de l'ordre des bits,
- recalcul du FCS,
- ne pas tenir compte de la priorité,
- acquitter la trame (bit A et C), alors que la station destinataire n'est peut-être pas à l'écoute,
- les buffers devront être suffisamment dimensionnés si le 802.5 est à 16 Mbit/s et que le réseau Ethernet est quelque peu chargé (congestion).

14.2 Spanning Tree Protocol (STR)

La démarche consiste à déterminer d'abord le pont racine, puis à calculer les différents coûts à partir de la racine.

1) Première solution

Le pont P1, de plus petit ID, est désigné comme pont *root* (racine). Sur chaque branche, il est très aisé de déterminer le pont élu, c'est celui de moindre coût. La seule difficulté qui subsiste concerne le pont P7. La figure 20.49 représente cet état intermédiaire.

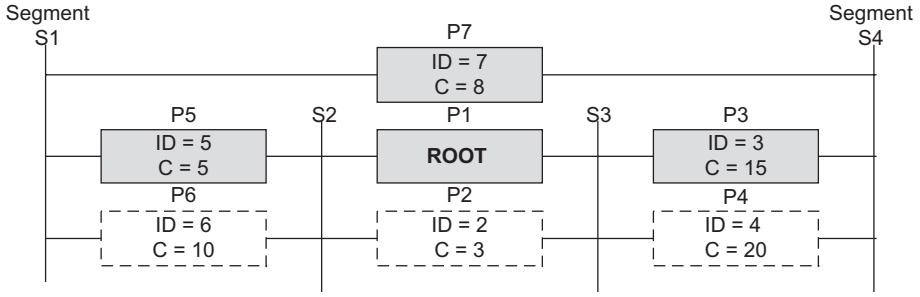


Figure 20.49 Solution intermédiaire.

La figure 20.50 cumule les coûts des différentes branches par lesquelles il est possible d'atteindre le port non-root du pont P3. Le coût en sortie de P3 est de 15, alors que ce port P3 reçoit une BPDU qui affiche un coût de 13. P3 en déduit qu'il existe un chemin moins cher pour atteindre cette direction, il se met en sommeil (pont *backup*).

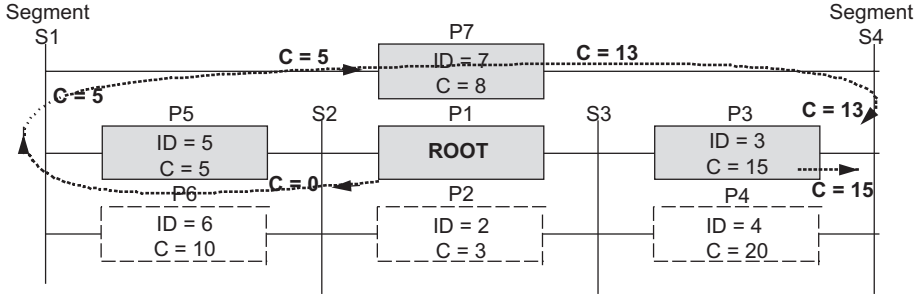


Figure 20.50 Détermination des coûts sur les branches de P7.

© Dunod – La photocopie non autorisée est un délit

Le schéma final, après stabilisation, est donné par la figure 20.51. L'examen de la topologie obtenue montre que le pont P5 doit écouler tout le trafic, il constitue donc le maillon sensible du réseau (débit, fiabilité...).

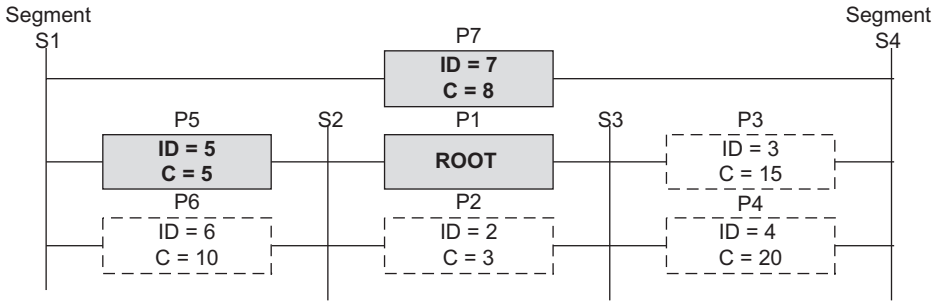


Figure 20.51 Configuration finale du réseau.

Cet état de fait, s'il n'est volontaire (coût des liens, conditions particulières d'exploitation, etc.), provient soit d'un mauvais choix du pont *root*, soit d'une mauvaise affectation des coûts.

2) Deuxième solution

Le schéma de la figure 20.52 propose une alternative devant conduire à une topologie équilibrée.

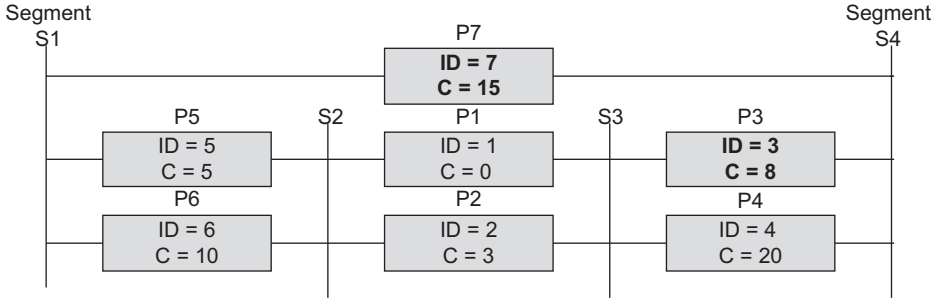


Figure 20.52 Nouvelle définition du réseau.

La figure 20.53 donne la topologie finale du réseau. Les trafics sont mieux répartis.

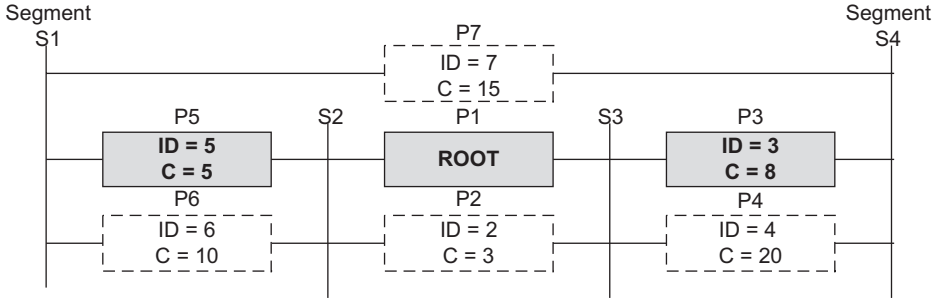


Figure 20.53 Nouvelle configuration du réseau.

La figure 20.54 fournit une représentation différente. Celle-ci montre l'arborescence des différentes branches et situe les voies de secours (*backup*).

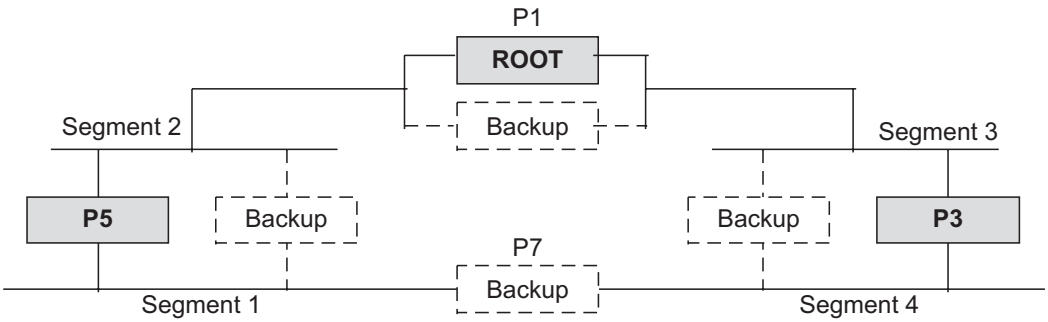


Figure 20.54 Arbre représentatif du réseau final.

14.3 Protocoles RIP/OSPF

Les principaux éléments de comparaison entre le protocole RIP et OSPF sont indiqués figure 20.55.

	RIP	OSPF
Caractéristiques		
Type d'algorithme	Vecteur distance	État des liens
Métrique	Nombre de sauts	Coût de la liaison
Métrique configurable	Non	Oui
Origine	IETF	IETF
Architecture du réseau		
Type	À plat	Hiérarchique
Nombre de routeurs	15	Illimité
Routeur maître	Non	Oui
Support des masques de longueur variable	Non	OUI
Performance		
Charge du réseau	Élevée	Faible
Périodicité des mises à jour	30 secondes	3 minutes
Temps de convergence	Plusieurs minutes	Quelques secondes
Mode de mise à jour	Information du voisin	Multicast
Support de la qualité de service	Non	Oui
Sécurité		
Authentification	RIP-2	Mot de passe dans chaque paquet

Figure 20.55 Comparaison RIP/OSPF.

© Dunod – La photocopie non autorisée est un délit

14.4 Agrégation de routes

a) Nombre d'entrées dans la table du routeur de bordure d'aires du backbone sans l'agrégation de routes

À chaque sous-réseau correspond une entrée, le plan d'adressage représenté figure 20.56 indique 16 sous-réseaux par aire, soit un total de 48 entrées dans la table du routeur de bordure.

b) Annonces des routeurs de bordure d'aires (figure 20.56)

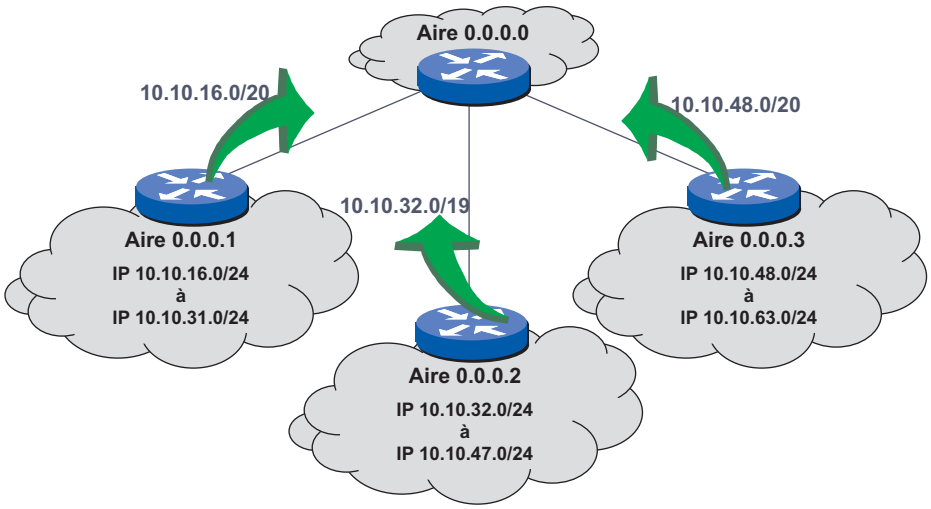


Figure 20.56 Comparaison RIP/OSPF.

Les annonces correspondent au plus petit masque de sous-réseau commun à tous les sous-réseaux de la zone (adresses contiguës de sous-réseaux). Pour cela nous examinerons l'expression binaire de chacune des adresses réseau (dernier octet d'adresse)

– Aires 1 :

10.10.16.0/24 → 000**1** 0000

10.10.17.0/24 → 000**1** 0001

...

10.10.31.0/24 → 000**1** 1111

Soit la plus petite annonce commune 10.10.16.0/20

– Aires 2 :

10.10.32.0/24 → 00**1**0 0000

10.10.33.0/24 → 00**1**0 0001

...

10.10.47.0/24 → 00**1**0 1111

Soit la plus petite annonce commune 10.10.32.0/19

– Aires 3 :

10.10.48.0/24 → 00**11** 0000

10.10.49.0/24 → 00**11** 0001

...

10.10.63.0/24 → 00**11** 1111

Soit la plus petite annonce commune 10.10.48.0/20

c) Ordre des entrées dans la table

Afin d'éviter toute ambiguïté les adresses, dont le masque est le plus important, sont classées en tête soit :

10.10.48.0/20

10.10.16.0/20

10.10.32.0/19

14.5 Adresses multicast

Indépendamment de l'abonnement à un groupe multicast l'adaptateur Ethernet répond aux adresses suivantes :

– son adresse unicast : 08-00-02-2D-75-BD ;

– l'adresse de broadcast : FF-FF-FF-FF-FF-FF ;

Si la station s'abonne au groupe multicast 224.16.21.5, l'adaptateur répondra aussi à l'adresse MAC multicast construite à partir de l'adresse de diffusion du groupe multicast. Cette adresse est la résultante de la somme de l'adresse MAC réservée 01-00-5E-00-00-00 et des 23 derniers bits de l'adresse de diffusion du groupe (figure 20.57) :

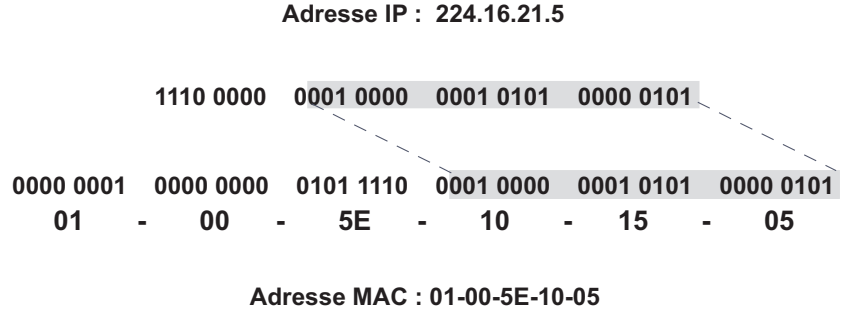


Figure 20.57 Construction de l'adresse multicast.

14.6 Comparaison pont/routeur

Le tableau de la figure 20.58 fournit les différents critères de comparaison entre un pont et un routeur.

© Dunod – La photocopie non autorisée est un délit

	Pont	Routeur
Configuration	Très simple (voire sans)	Complexe
Transparence aux protocoles	Oui	Non (Protocoles routables)
Sécurité (Filtre)	Sur adresse MAC	Sur adresse IP (Masque)
Extension du réseau	Aisée	Complexe si routage statique
Trafic de service	Sans, sauf Spanning Tree	Oui, pénalisant
Broacast	Transparent	Filtre, sauf broadcasts dirigés
Charge de travail (personnel)	Négligeable	Importante

Figure 20.58 Comparaison Pont/Routeur.

14.7 Masque de sous-réseau

Les deux stations du réseau représenté figure 20.59 ne peuvent correspondre puisqu'elles sont, vis-à-vis du masque de sous-réseau sur le même réseau.

Figure 20.59 Réseau défaillant.

Soit il s'agit d'une erreur de configuration d'une des stations qu'il suffit alors de corriger, soit d'une erreur dans la définition du masque de sous-réseau qui porté à 24 bits distinguerait alors deux sous-réseaux distincts.

14.8 Routage statique

Chaque entrée contient l'adresse réseau de la machine destination, la prochaine adresse distante de la route locale à prendre (adresse de l'extrémité distante de la liaison ou *Next Hop*) et les masques associés. Le routeur détermine le port de sortie à prendre par comparaison du Net_ID de la LS distante et du Net_ID de ses différents ports (adresses locales des LS).

Les tables d'extrémité sont les plus simples, les routeurs d'extrémité (Brest et Strasbourg) n'ont qu'à envoyer tout ce qu'ils reçoivent vers le centre de l'étoile (Paris). La table du nœud de Paris ne présente aucune difficulté particulière. La plus complexe est celle du nœud de Marseille qui doit tenir compte des deux sous-réseaux (figure 20.60).

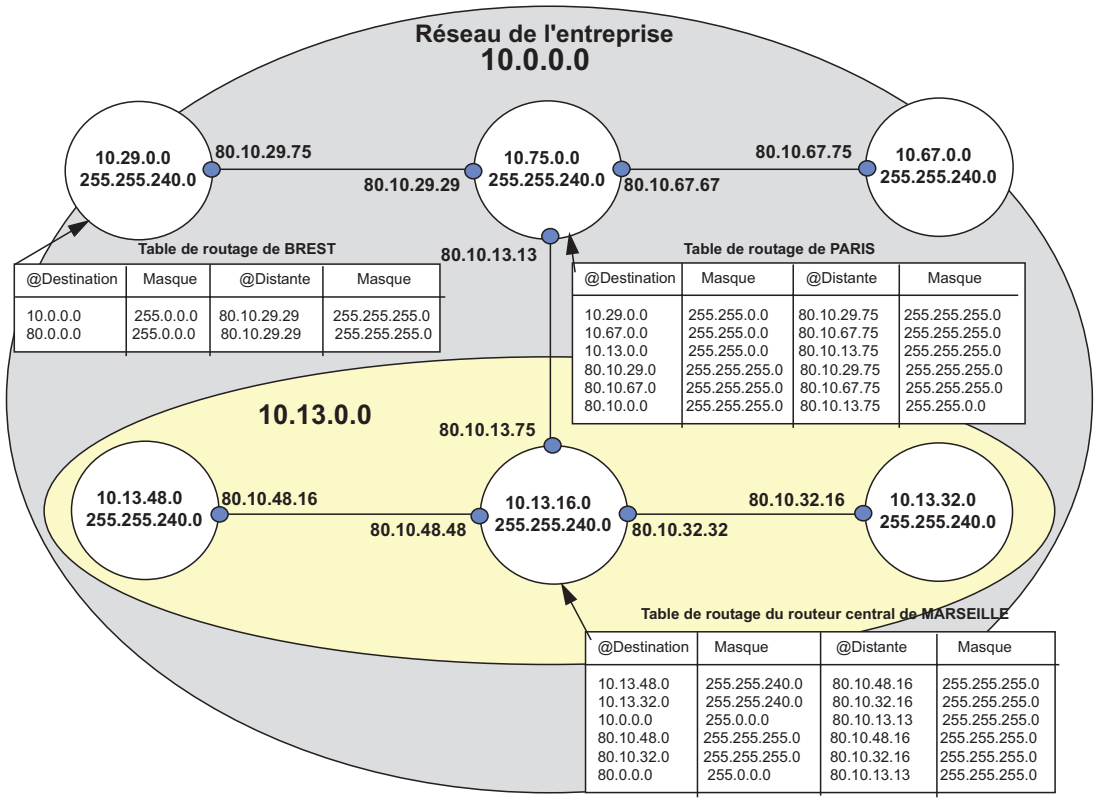


Figure 20.60 Tables de routage.

CHAPITRE 15

15.1 Capacité d'un autocommutateur

Le trafic total est la somme du trafic résidentiel et du trafic professionnel soit :

$$\text{Trafic Total (Tt)} = \text{Trafic Résidentiel (Tr)} + \text{Trafic professionnel (Tp)}$$

Si x est le nombre d'abonnés on a :

$$\text{Tr} = 0{,}1 \times 0{,}4x \qquad \text{et} \qquad \text{Tp} = 0{,}3 \times 0{,}6x$$

Soit

$$5\,000 = 0{,}1 \times 0{,}4x + 0{,}3 \times 0{,}6x \qquad \text{donc} \qquad x = 5\,000/0{,}22 = 22\,727$$

Le nombre d'abonnés reliés à l'autocommutateur est de 22 727.

© Dunod – La photocopie non autorisée est un délit

15.2 Itinérance

Les causes de rupture de communication sont nombreuses, citons :

– mobile dans une zone d'ombre ;

– batterie trop faible ;

– vitesse de déplacement du mobile trop importante ;

– mobile en limite de portée d'une cellule et plus de capacité d'accueil dans la cellule qui aurait dû, compte tenu de la position du mobile, le prendre en charge.

15.3 Système Iridium

Le système Iridium utilise 66 satellites répartis sur 6 orbites soit 11 satellites par orbite. Le temps de couverture moyen d'un satellite correspond au temps qui sépare le passage de 2 satellites successifs. Durée de visibilité d'un satellite : Période de révolution/nombre de satellites = 100/11 = 9 mn.

Nota : la durée réelle de visibilité est de 11 mn.

15.4 Schéma de réutilisation des fréquences

Le schéma minimal de réutilisation des fréquences est de 3 (figure 20.61). Dans ces conditions chaque cellule peut utiliser 240/3 soit 80 fréquences.

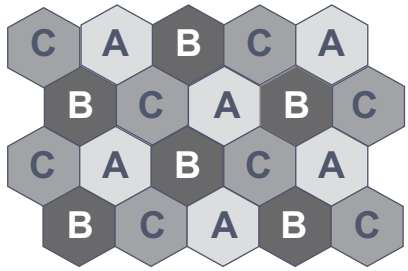


Figure 20.61 Schéma de réutilisation des fréquences (motif de 3).

15.5 Protocole D (Q.931)

Analyse du renvoi du poste vers le 01 23 45 67 89

a) Diagramme des échanges (figure 20.62)

Le diagramme des échanges est simple. Le plus intéressant dans cet exercice est le décodage des messages transmis que nous détaillerons complètement. Le décodage de ces messages montre la complexité et la richesse de la signalisation Q.931.

Le poste TEI 64 reçoit le message d'établissement (adresse de diffusion TEI 127) en provenance du réseau. Le poste, renvoyé sur le 01 23 45 67 89, demande l'établissement d'une connexion pour acheminer son message de renvoi (SABME). La connexion étant acceptée par le réseau (UA), le message de renvoi est adressé au réseau (Trame d'INFO).

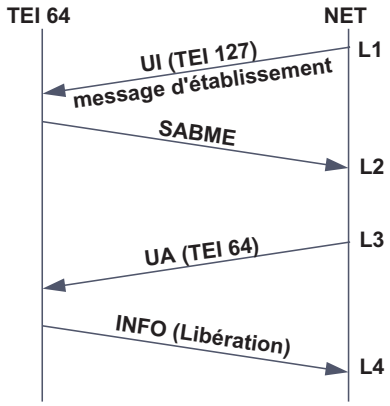


Figure 20.62 Diagramme des échanges sur renvoi d'un poste.

b) Analyse des éléments d'information

Message d'établissement : le message d'établissement est envoyé par l'usager appelant ou le réseau pour initialiser l'établissement d'un appel. Il comprend toutes les informations nécessaires à l'établissement de la connexion et à l'exécution du service demandé.

L'élément d'information « **mode de fonctionnement du support** » a pour objet d'indiquer le mode de fonctionnement demandé pour le support, l'ensemble des éléments d'information est transmis de bout en bout.

80h	1-------	Ce bit, dit bit d'extension est toujours à 1 pour les éléments d'information.
	-00-----	Indique la norme de codage, ici codage CCITT, les autres valeurs ne sont pas attribuées (réservées pour une utilisation future).
	---00000	Précise le mode de fonctionnement du transfert d'information. Les valeurs suivantes sont utilisées :
		00000 Parole (communication téléphonique).
		00100 Informations numériques.
		01000 3,1 kHz acoustique.
90h	1-------	Extension Bit
	-00-----	Cette information précise le mode de transfert des informations, seule la valeur 00 est utilisée. Les autres valeurs sont réservées.
	---10000	Indique le débit de transfert des informations, seule la valeur 10000 est utilisée (64 kbit/s).
A3h	1-------	
	-01-----	Identifie la couche et le protocole, 01 (seule valeur utilisée) indique le protocole de la couche 1 d'information usager utilisé, précisé dans les bits suivants.
	---00011	Seule valeur utilisée, elle indique que le codage du signal suit la recommandation G.711 loi A.

L'élément d'information « **Identification du canal** » identifie un canal à l'interface usager/réseau.

© Dunod – La photocopie non autorisée est un délit

81h `1-------` Ce bit, dit bit d'extension est toujours à 1 pour les éléments d'information.

`-0------` La valeur 0 indique que l'interface est explicitement identifiée. La valeur 0 est réservée.

`--0-----` Précise le type d'interface usager, 0 interface de base, 1 interface débit primaire.

`---0----` Non utilisé, réservé.

`----0---` Indique si le canal spécifié est préféré ou obligatoire (exclusif). La valeur 0 indique que le canal est seulement préféré, tandis que la valeur 1 indique que seul le canal spécifié est acceptable.

`-----0--` Précise si c'est le canal D qui est requis (1). 0 ce n'est pas le canal D. La valeur 1 est réservée.

`------01` Sélection de canal, précise le canal requis :

00 Pas de canal
01 Canal B1
10 Canal B2
11 N'importe quel canal.

L'élément d'information « **Compatibilité de la couche supérieure** » permet au demandé de vérifier la compatibilité du terminal avec le téléservice demandé.

D1h `1-------` Bit d'extension, toujours à 1.

`-10-----` Précise les normes de codage utilisées.

00 Norme CCITT
10 Norme CEPT ou national (précisé par le bit 5)

`---100--` Interprétation

000 norme nationale
100 CCITT/CEPT

`------01` Présentation, 01 seule valeur attribuée, la méthode utilisée pour préciser le service est la méthode du profil.

81h `1-------`

`-0000001` Indication du téléservice demandé :
Norme CCITT.

0000001 Téléphone
0000100 Télécopie groupe 3
0100001 Télécopie groupe 4
0100100 Télétex mode mixte
0110001 Télétex mode caractère
0110010 Vidéotex alpha-mosaïque
0110101 Télex
0111000 Système de traitement de message (STM)
1000001 Application ISO

Message de libération : ce message signale que l'équipement a déconnecté le canal et qu'il a libéré les références d'appel. Le récepteur doit procéder de même, et éventuellement interrompre tout appel en cours.

L'élément d'information « **Cause** » est obligatoire, il précise la raison pour laquelle a été émis le message.

87h `1-------` Bit d'extension, toujours à 1.

`-00-----` Indique les normes appliquées, seule valeur 00 (CCITT). Les autres valeurs sont réservées.

`---00---` Toujours 00.

`-----111` Localisation, 111 non significatif, à mettre en relation avec la cause de la libération. Toutes les autres valeurs sont réservées.

90h `1-------` Bit d'extension, toujours à 1.

`-001----` La cause est codée sur 2 champs. Le premier représente la classe de l'erreur :

- **001 Situation normale.**
- 010 Encombrement temporaire du réseau.
- 011 Service ou option non disponible.
- 100 Service ou option non mis en œuvre.
- 101 Message non valide (ex : paramètre, hors gamme)
- 110 Erreur de protocole (ex : message inconnu).
- 111 Interfonctionnement.

`----0000` La valeur de l'erreur est précisée ici :

- **0000 Libération normale.**
- 0001 Usager occupé.
- 0010 Pas de réponse de l'usager.
- 0011 Complément de service non enregistré.
- 0101 Rejet de l'appel.
- 0110 Numéro changé.
- 1000 Numéro non attribué.
- 1011 Destination hors service.
- 1100 Adresse incomplète.
- 1111 Normal non spécifié.

L'élément d'information « **Facilité** » indique les compléments de service demandés. Cet élément est codé sur une longueur comprise entre 4 et 24 octets.

00h `00000000` Longueur de l'identification du réseau, toujours à 0.

2Ah `00101010` soit « · » Préfixe du code service demandé, obligatoire dans le sens usager/réseau.

- **00101010 · Activation ou enregistrement de service**.
- 00100011 # Désactivation ou annulation d'un service.
- ·# Fonction d'interrogation de l'enregistrement d'un service.

© Dunod – La photocopie non autorisée est un délit

32h Demande d'indication d'appel malveillant : « ·32# ».
23h « # » Fin du champ complément de service.

L'élément d'information « **Mode de fonctionnement usager** » permet aux terminaux de préciser au réseau leur mode de fonctionnement.

80h `10------` Norme de codage, seule valeur attribuée 10, norme nationale.
`--000000` Description du mode de fonctionnement, seule valeur attribuée 000000, terminal en mode de fonctionnement national.

L'élément d'information « **numéro destination** » identifie la destination de l'appel.

80h `1-------` Bit d'extension, toujours à 1.
`-000----` Type de numéro appelé :
000 Numérotation en bloc.
101 Envoi par chevauchement.
Les autres valeurs sont réservées.
`----0000` Indique le plan de numérotation utilisé :
0000 plan inconnu.
1001 plan de numérotation privé.
Les autres valeurs sont réservées.

30 31 32 33 34 35 36 37 38 39 : codage du numéro appelé en format IA5 (Alphabet international N°5).
Ce qui se lit directement : 01 23 45 67 89.

CHAPITRE 16

16.1 Utilisation de l'abaque d'Erlang

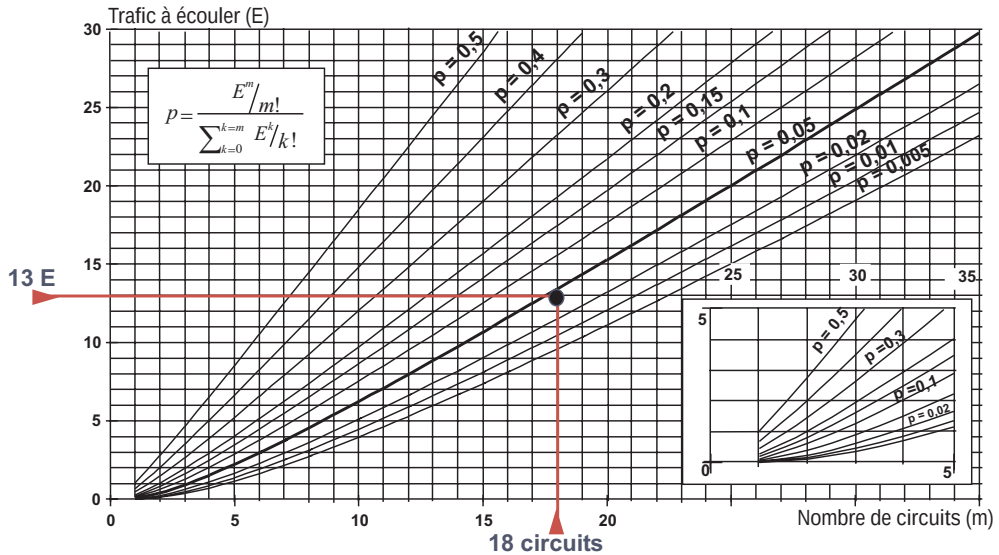


Figure 20.63 Utilisation de l'abaque d'Erlang.

Rappelons que l'abaque à refus fournit pour un trafic à écouler de ***E*** erlang par un système de ***M*** ressources, le taux de perte de trafic. Ainsi, la figure 20.63 montre que si on soumet un trafic de 13 E à un système disposant de 18 circuits, le taux de refus est d'environ 5%.

Sachant que Trafic perdu = Trafic soumis – Trafic écoulé

Probabilité de perte	**1%**			**10%**			**50%**		
Nb. circuits	Soumis	Perdu	Ecoulé	Soumis	Perdu	Ecoulé	Soumis	Perdu	Ecoulé
5	1,25	0,02	1,23	3	0,3	2,7	9,5	4,75	4,75
10	4,5	0,05	4,45	7,5	0,75	6,75	18,5	9,25	9,25
15	8	0,08	7,92	12,5	1,25	11,25	28,5	14,25	14,25

Figure 20.64 Différents trafics sur un faisceau.

16.2 Trafic sur un faisceau

Un circuit pouvant écouler 1 E, le rendement d'un circuit est le rapport entre le trafic réellement écoulé par un circuit et le trafic unitaire (1 E). La lecture de l'abaque donné en annexe permet de remplir le tableau ci-après (figure 20.65).

Nb circuits par faisceau	**Trafic soumis**	**Trafic écoulé**	**η par circuit**
10	6 E	5,7	0,57
$2 \cdot 10$	12 E	11,4	0,57
20	15 E	14,25	0,71

Figure 20.65 Rendement d'un faisceau.

Plus un faisceau est petit, plus les risques de collision d'appel sont importants, donc pour une même probabilité d'échec un rendement par circuit plus petit.

16.3 Raccordement d'un PABX

1) Capacité de commutation du PABX

Le PABX doit assurer l'écoulement de tous les types de trafic pour tous les postes qui y sont raccordés soit :

$$C = \text{Trafic d'un poste} \times \text{Nombre de postes}$$

$$C = 0{,}12 \text{ E} \times 120 = 14{,}4 \text{ erlangs}$$

Capacité du PABX : 14,4 erlangs

2) Faisceau SPA, compte tenu d'un taux de refus inférieur à 10 %

En cas d'occupation, les appels sortants sont refusés, c'est l'abaque à refus qu'il convient d'utiliser.

Trafic sortant à écouler :

$$T = 0{,}04 \times 100 = 4 \text{ E}$$

La lecture de l'abaque d'Erlang à refus (en annexe) indique que 7 circuits sont nécessaires.

© Dunod – La photocopie non autorisée est un délit

3) Faisceau SPB, compte tenu d'une mise en attente inférieure à 2 %

En cas d'indisponibilité du correspondant, aucun trafic n'est écoulé pendant que le demandeur occupe un circuit (musique d'attente). Dans ces conditions, c'est l'abaque à attente qu'il convient d'utiliser (en annexe).

Trafic à écouler :

$$T = 0{,}004 \times 100 = 4 \text{ E}$$

La lecture de l'abaque d'Erlang à attente (en annexe) indique que 9 circuits sont nécessaires.

16.4 Trafic d'un centre d'appel

Le traitement d'une communication dure 30 s (25 + 5) soit une capacité de traitement de 2 appels/minute. Une ligne (1 erlang) est donc capable de recevoir 120 appels/heures. Sachant que le trafic à écouler est de 360 000 appels/heure (720 000/2), le nombre de lignes nécessaires est de : 360 000/120 = 3 000 lignes soit aussi 3 000 erlangs.

16.5 Réseau voix/données

a) Nombre de canaux voix utilisables

Au-dessus d'une charge supérieure à 50 %, le temps de transit dans les files d'attente augmente rapidement. Afin de garantir une gigue de paquets minimale, la file d'attente voix ne devra pas être chargée à plus de 50 %. Compte tenu de l'utilisation d'un algorithme de compression à 16 kbit/s, un lien à 64 kbit/s ne pourra supporter plus de 2 canaux voix.

b) Bande passante disponible

La bande occupée par un canal voix est égale au produit de la taille de la trame Frame Relay par le nombre de trames/s. La taille de la trame voix est égale à la taille du paquet voix à laquelle il convient d'ajouter les données protocolaires.

Taille d'un paquet voix – les systèmes utilisant la compression ADPCM à 16 kbit/s émettent une trame toutes les 20 ms (50 trames/s), correspondant au transport de :

Débit nominal/fréquence de récurrence $= 16\,000/50 = 320$ bits/trame

Taille d'un paquet sans en-tête $= 320/8 = 40$ octets

Débit disponible pour les données – l'encapsulation FRF11 ajoute 2 octets (voir figure 16.46), le protocole Frame Relay ajoute 6 octets (2 fanions, 2 DLCI, 2 FCS), la trame voix est de 40 + 2 + 6 = 48 octets.

– Bande nécessaire pour un canal voix (1 trame toutes les 20 ms, soit 50 trames/s) :

$$48 \times 8 \times 50 = 19\,200 \text{ bit/s}$$

– Pour 2 canaux voix :

$$19\,200 \times 2 = 38\,400 \text{ bit/s}$$

– Bande disponible pour les données :

$$64\,000 - 37\,600 = 25\,600 \text{ bit/s}$$

Remarque : Ce résultat ne tient pas compte des bits de transparence.

c) Taille maximale des paquets de données

Le débit maximal utilisable étant de 25 600 bit/s, ce débit pouvant être écoulé à raison de 50 trames/seconde, la taille d'une trame est de : $25\,600/50 = 512$ bits soit 64 octets. Cette valeur correspond à une valeur couramment utilisée dans les systèmes, elle sera retenue comme taille de charge utile. Compte tenu des données d'en-tête il convient d'ajouter les 8 octets (6 + 2) d'encapsulation soit 72 octets. La figure 20.66 représente la « trame multiplexée » sur le support WAN.

Figure 20.66 Entrelacement voix/données.

Notons que le débit maximal soumis au lien peut être de $(48+48+72) \times 8 \times 50 = 67\,200$ kbit/s (lien à 64 kbit/s) !

d) Gigue d'insertion

La gigue sera maximale quand un paquet de données sera émis juste avant l'arrivée d'un paquet voix. Ce dernier devra attendre la fin d'émission du paquet de données. Cela correspond donc au temps d'émission d'un paquet de données : Volume/Débit $= 72 \times 8/64\,000 = 9$ ms par lien traversé.

Si le bilan temps du réseau montre que cette gigue est trop importante, il conviendra de réduire la taille des paquets de données, où plus logiquement d'augmenter le débit du lien !

16.6 Dimensionnement d'un réseau Frame Relay voix/données

DLCI voix

La compression ADPCM à 16 kbit/s émet une trame toutes les 20 ms (50 trames/s), ce qui correspond au transport de :

Débit nominal/fréquence de récurrence $= 16\,000/50 = 320$ bits/trame

Taille d'un paquet sans en-tête $= 320/8 = 40$ octets

L'encapsulation FRF11 ajoute 2 octets (voir figure 16.46), le protocole Frame Relay ajoute 6 octets (2 fanions, 2 DLCI, 2 FCS), la trame voix est de 40 + 2 + 6 = 48 octets.

Le débit minimal (CIR) nécessaire à 1 canal voix est de $48 \times 8 \times 50 = 19\,200$ bit/s.

Les paquets voix doivent être transportés sans être rejetés, le calcul précèdent ne tient pas compte des bits de transparence. Il est malheureusement impossible de déterminer le volume supplémentaire introduit par la transparence. Arbitrairement nous arrondirons le débit requis au kbit supérieur, soit un CIR pour le DLCI voix de :

$$19\,200 \times 2 = 38\,400 \text{ bit/s arrondi à 40 kbit/s}$$

Par contre, il n'est nullement besoin de définir un trafic excédentaire (EIR=0). Les caractéristiques du DLCI voix seront :

CIR = 40 000 bit/s (sur réseau public 48 000 bit/s)

EIR = 0

© Dunod – La photocopie non autorisée est un délit

DLCI signalisation

La signalisation est fournie par le PABX, quand des informations de signalisation sont émises, elles le sont au débit du lien PABX/VFRAD en conséquence seul un CIR est à déterminer. De même pour tenir compte des bits de transparence, on arrondira au kbit supérieur soit :

$\text{CIR} = 10\,000\ \text{bit/s}$

$\text{EIR} = 0$

En l'absence d'information de signalisation, toute la bande passante pourra être récupérée par l'EIR du DLCI données.

DLCI données

La donnée pourra utiliser toute la bande restante soit $128\,000 - 40\,000 - 10\,000 = 78\,000\ \text{bit/s}$. Les caractéristiques du DLCI données seront fixées à :

$\text{CIR} = 78\ \text{kbit/s}$

$\text{EIR} = 128 - 78 = 50\ \text{kbit/s}$

Le débit réel de la donnée sera largement supérieur au CIR, le canal données pouvant profiter de la récupération des silences (50 à 60 % de la bande) et de l'absence d'information de signalisation.

16.7 Comparaison H.323 et SIP

Critères	H.323	SIP
Normalisation	UIT H.323 V4	IETF RFC 2543
Transport de la signalisation	TCP	TCP/UDP
Transport des flux multimédia	UDP	TCP/UDP
Établissement de canaux logiques	Oui, un par sens	Non
Signalisation multicast	Non	Oui
Prioritisation des appels	Non	Oui
Codage des primitives	Binaire Interopérabilité facilitée	Texte Décodage simplifié
Evolutivité	Faible, beaucoup d'extensions propriétaires	Protocole ouvert
Détection des boucles	Non, pas dans la V1	Oui
Gestion des conférences	Centralisée (MCU)	Distribuée

Figure 20.67 Comparaison H.323 et SIP.

CHAPITRE 17

17.1 MTTR/MTBF

Calcul de la disponibilité

Étape 1 : Pour calculer la disponibilité et l'indisponibilité de l'ensemble, il faut déterminer la disponibilité et l'indisponibilité de chacun de ses composants.

	MTBF	MTTR	Disponibilité (A)	Indisponibilité (I)
Système 1 & 2	4 mois	8 heures	(4 x 200)/(4 x 200 + 8) = 0,99	1 – 0,99 = 0,01
Modem	2 ans	5 heures	(2 400 x 2)/(2 400 x 2 + 5) = 0,9989	1 – 0,9989 = 0,0011
RTC	2 ans	24 heures	(2 400 x 2)/(2 400 x 2 + 24) = 0,9950	1 – 0,9950 = 0,005
Telcos	2 ans	2 heures	(2 400 x 2)/(2 400 x 2 + 2) = 0,9995	1 – 0,9995 = 0,0005

Figure 20.68 Disponibilité et indisponibilité.

Étape 2 : Établissement du diagramme de fiabilité du système

À chaque élément du système, on substitue une représentation quantifiée de sa disponibilité et de son indisponibilité. En remplaçant la représentation fonctionnelle par une représentation basée sur les structures élémentaires, on obtient un diagramme qu'il suffit de simplifier, en y appliquant les règles de regroupement des structures élémentaires, pour déterminer la disponibilité et l'indisponibilité globales du système étudié.

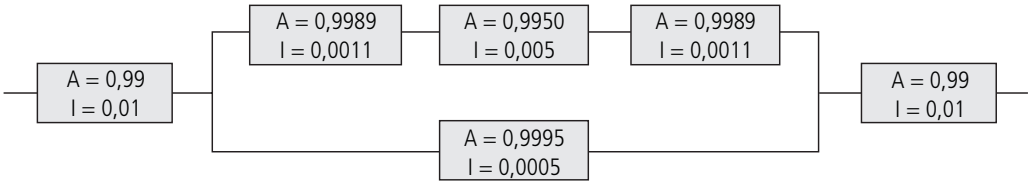


Figure 20.69 Diagramme de fiabilité.

Étape 3 : On formalise par branche

– Branche 1 : Modem-RTC-Modem

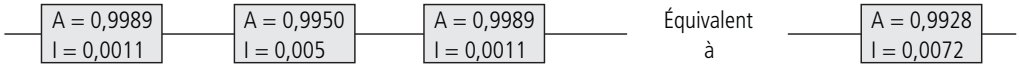


Figure 20.70 Étude de la branche Modem-RTC-Modem.

$$A_t = A_1 \cdot A_2 \cdot \ldots \cdot A_n = 0{,}9989 \cdot 0{,}9950 \cdot 0{,}9989 = 0{,}9928$$

$$I_t = 1 - A_n = 0{,}0072$$

où $I_t = \Sigma\, I = 0{,}0072$

– Branche 2 : Branche 1 en parallèle avec le réseau de l'opérateur

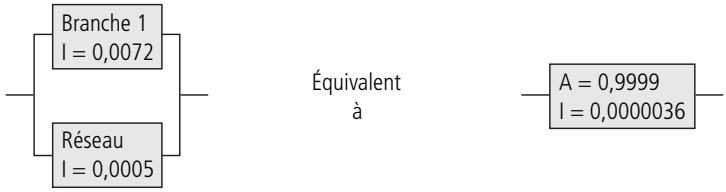


Figure 20.71 Branche 1 et réseau de l'opérateur.

$$I_t = I_1 \cdot I_2 \cdot \ldots \cdot I_n = 0{,}0072 \cdot 0{,}0005 = 0{,}0000036$$

$$A_t = 1 - I_n = 0{,}9999$$

© Dunod – La photocopie non autorisée est un délit

– Branche 3 : Système 1– Branche 2 – Système 1 (structure finale)

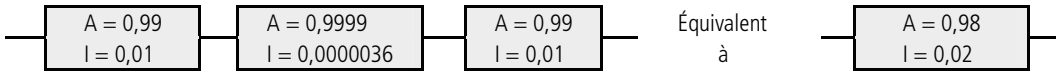


Figure 20.72 Structure finale.

$A_t = A_1 \cdot A_2 \cdot .... \ A_n = 0{,}99 \cdot 0{,}9999 \cdot 0{,}99 = 0{,}98$

$I_t = 1 - A_n = 0{,}02$

$I_t = \Sigma\, I = 0{,}0072$

Interprétation des résultats : La disponibilité du système est de 98 %, c'est-à-dire qu'il y aura 98 heures de bon fonctionnement et 2 heures de panne en moyenne pour 100 heures de mise à disposition des équipements, mais cette valeur globale n'indique nullement l'espérance de bon fonctionnement entre 2 pannes. Pour cela, il nous faut déterminer la MTBF et la MTTR résultante.

Calcul de la MTBF/MTTR

Le calcul est équivalent, reprenons à partir de l'étape 3.

Étape 3 : On formalise par branche

– Branche 1 : Modem -RTC-Modem

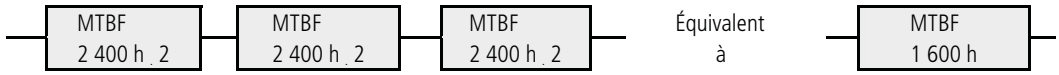


Figure 20.73 Branche Modem-RTC-Modem.

$MTBF = 1/\Sigma_{i=1\ à\ n}\ (1/MTBF_i)$

$MTBF = 1/(1/4\,800 + 1/4\,800 + 1/4\,800) = 4\,800/3 = 1\,600$ h

I/A = MTTR/MTBF soit MTTR = (I/A) × MTBF

MTTR = (0,0072 × 1 600)/0,9928 = 11,60 h

– Branche 2 : Branche 1 en parallèle avec le réseau opérateur,

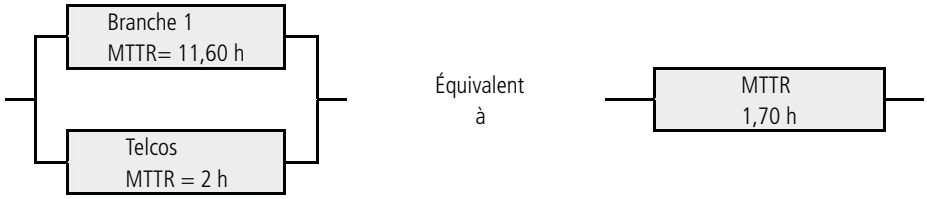


Figure 20.74 Branche 1 et réseau de l'opérateur.

$MTTR = 1/\Sigma_{i=1\ à\ n}\ (1/MTTR_i)$

MTTR = 1/(1/11,60 + 1/2) = 1,70 h

I/A = MTTR/MTBF soit MTBF = (A/I) × MTTR

MTBF = (0,9999 × 1,70)/0,0000036 = 472 175 h

– Branche 3 : Système 1– Branche 2 – Système 1 (structure finale)

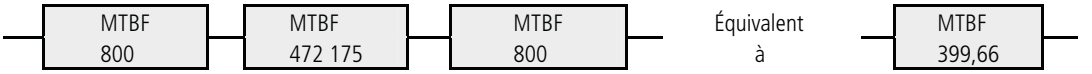


Figure 20.75 Structure finale.

$MTBF = 1/\Sigma_{i=1 \text{ à } n} (1/MTBF_i)$

$MTBF = 1/(1/800 + 1/472\,175 + 1/800) = 399{,}66$ h

I/A = MTTR/MTBF soit MTTR = (I/A) × MTBF

$MTTR = (0{,}02 \times 399{,}66)/0{,}98 = 8{,}15$ h

Ce qui correspond à une immobilisation d'une journée environ tous les deux mois.
Vérification :

$$A = MTBF/(MTBF + MTTR) = 399/(399 + 8{,}15) = 0{,}98.$$

17.2 Systèmes à clés symétriques ou secrètes

Dans un système à clés secrètes comportant N utilisateurs, chaque utilisateur doit connaître sa clé et celle de ses $N - 1$ correspondants potentiels. Ce qui correspond pour un utilisateur à N clés soit pour le système N^2 clés à gérer.

Dans un système à clé publique, chaque utilisateur n'a à connaître que la clé publique de ses $N - 1$ correspondants potentiels et sa propre clé secrète soit N clés.

17.3 Algorithme à translation de César

Plusieurs approches sont envisageables pour déchiffrer un crypte. En supposant connu l'algorithme de chiffrement utilisé, on peut essayer toutes les clés possibles. Cette méthode est évidemment peu efficace. On peut, connaissant l'origine du texte, tenter de retrouver un mot spécifique au contexte... La méthode la plus simple vis-à-vis de l'algorithme de César est de repérer la lettre dont l'apparition est la plus importante et de supposer successivement que cette lettre est le crypte de la lettre E, A, I, O, S... dans l'ordre de la fréquence d'apparition des lettres dans la langue considérée. En appliquant cette méthode au crypte « HTIFLJIJHJXFW », la lettre J ayant la plus grande apparition sera d'abord supposée correspondre au clair E, soit une translation de 5. Ce qui correspond à la grille ci-dessous :

Clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Crypte	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Figure 20.76 Table de translation.

Soit le texte clair : « Codage de César »

© Dunod – La photocopie non autorisée est un délit

17.4 Algorithme de substitution de Vigenère

Méthode :

a) Recopier autant de fois que nécessaire la clé. Afin d'obtenir un texte de longueur identique à celle du crypte (figure 20.77).

b) Déterminer la lettre du clair en pratiquant comme suit : à partir de la lettre de la clé, on recherche dans la colonne la lettre du crypte. En lisant horizontalement, on obtient la lettre du clair (figure 20.77).

c) Lire et réintroduire les blancs.

Clé	S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E
Crypte	L	E	D	C	I	T	M	H	G	M	M	Z	W	R	G	I	I
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Clair	T	A	B	L	E	A	U	D	E	V	I	G	E	N	E	R	E

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	↓ 19	20	21	22	23	24	25	26
	1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	**S**	T	U	V	W	X	Y	Z
	2	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K	R	S	T	U	V	W	X	Y	Z	A
	3	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	4	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	5	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	6	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	7	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	B	E	F
	8	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y	Y	Z	A	B	C	D	E	F	G
	9	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	10	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	11	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	12	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	13	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	14	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	15	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	16	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	17	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	18	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K
	19	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K	R
←	20	**T**	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	**L**	M	N	O	P	Q	R	S
	21	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	22	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	23	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K	R	S	T	U	V
	24	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	25	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	26	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 20.77 Mise en correspondance de la clé, du crypte et du clair.

Le clair est donc « Tableau de Vigenère ».

17.5 Algorithme du RSA

Rappels de l'algorithme du RSA

Le système de cryptographie à clé asymétrique le plus répandu, le RSA, repose sur l'arithmétique des grands nombres. La fonction de chiffrement est de la forme :

$$\text{Crypte} = \text{Clair}^{\text{clé C}} \text{ modulo } n$$

Crypte : message codé, Clair : message à coder,
clé C : clé de chiffrement n : produit de nombres premiers.

La fonction de déchiffrement est identique :

$$\text{Clair} = \text{Crypte}^{\text{clé D}} \text{ modulo n}$$

Crypte : le message codé Clair : message à coder
clé D : la clé de déchiffrement n : produit de nombre premier.

L'algorithme de détermination des clés est rappelé ci-dessous :

1) Choisir deux nombres premiers p et q grands et différents ($> 10^{100}$).
2) Calculer n tel que $n = p \times q$.
3) Choisir les clés telles que $C \times D = 1 + M[(p-1) \times (q-1)]$, où M est un entier qui satisfasse l'égalité.
4) Définir la longueur maximale (L) du bloc de bits sur lequel on applique l'opération de sorte que $2^L < n$.

a) Recherche des plus petites clés possibles

Les nombres p, q devant être plus grands que 1, le premier couple de nombres premiers est 2, 3. Dans ces conditions :

$n = p \times q = 2 \times 3 = 6$

$z = (p-1)(q-1) = 2$

$C \times D = 1 + M \times 2$ soit, pour les valeurs de M :

M	1 + M x 2	C	D	Commentaires
1	3	1	3	Une clé de 1 est absurde
2	5			5, nombre premier
2	7			7, nombre premier
4	9	3	3	Les clés sont symétriques
5	11			11, nombre premier
6	13			13, nombre premier
7	15	3	5	Valeurs acceptables

Figure 20.78 Recherche du plus petit couple de clés ($p = 2, q = 3$).

© Dunod – La photocopie non autorisée est un délit

La longueur du crypte élémentaire est $2^L < n$ soit $2^2 < 6$.
Dans ces conditions, les différentes valeurs élémentaires (2 bits) sont 0, 1, 2, 3.

Clair	N = Clair^C	Crypte = N mod n	N = Crypte^D	Clair = N mod n
0	0	0		
1	1	1		
2	8	2		
3	27	3		

Figure 20.79 Table de chiffrement (C = 3, D = 7).

Ces valeurs sont trop petites, le crypte est identique au clair. Il faut choisir un autre couple. Le plus petit couple (p, q) suivant est : 2, 5.

$n = p \times q = 2 \times 5 = 10$

$z = (p - 1)(q - 1) = 4$

$C \times D = 1 + M \times 4$ soit les valeurs de M :

M	1 + M x 2	C	D	Commentaires
1	5			5, nombre premier
2	9	3	3	Les clés sont symétriques
3	13			13, nombre premier
4	17			17, nombre premier
5	21	3	7	Valeurs acceptables

Figure 20.80 Recherche des clés suivantes (p= 2 , q = 5).

La longueur du crypte élémentaire est $2^L < n$ soit $2^3 < 6$.
Dans ces conditions, les différentes valeurs élémentaires (3 bits) sont :

Clair	N = Clair^C	Crypte = N mod n	N = Crypte^D	Clair = N mod n
0	0	0	0	0
1	1	1	1	1
2	8	8	2 097 152	2
3	27	7	823 543	3
4	64	4	16 384	4
5	125	5	78 125	5
6	216	6	279 936	6
7	343	3	2 187	7

Figure 20.81 Table de chiffrement ($C = 3, D = 7$).

Indépendamment du fait que nombre de cryptes sont encore égaux au clair, on a pu vérifier qu'il était bien possible de coder avec une clé et de décoder avec une autre.

b) Rejet de la solution établie

Le couple de clés calculé est inacceptable pour crypter un fichier. En effet, la valeur 2 est cryptée 8, c'est-à-dire codée sur 4 bits. Le déchiffrement étant réalisé par bloc de 3 bits, un décalage se produira, le message décrypté sera illisible. En conséquence il faut, d'une part, imposer que le plus grand nombre à coder (n – 1, puisque l'opération est modulo n) ait pour longueur binaire L (L doit être tel que $2^L + 1 = n$) et, d'autre part, que L doit être différent de 8, car le codage d'un même octet donnerait toujours la même valeur.

c) Détermination des plus petites clés possibles et utilisables

1) Le couple p, q *doit répondre à la condition* $2^L + 1 = n = p \times q$

$2^L + 1$	p x q	Commentaires
$2^1 + 1 = 3$	1 x 3	z = 0, solution impossible
$2^2 + 1 = 5$	1 x 5	z = 0, solution impossible
$2^3 + 1 = 9$	3 x 3	Nombres identiques
$2^4 + 1 = 17$	Nombre premier	
$2^5 + 1 = 33$	3 x 11	Solution acceptable

Figure 20.82 Recherche du couple p, q.

2) Détermination des clés

$n = p \times q = 3 \times 11 = 33$

$z = (p - 1) \times (q - 1) = 2 \times 10 = 20$

$C \times D = 1 + M \times 20$

Les plus petites valeurs possibles sont pour M = 1 : C = 3, D = 7.

Les paramètres du logiciel de cryptographie seront donc C = 3, D = 7, L = 5, n = 33

3) Matrice de chiffrement

Clair	N = Clair^c	Crypte = N mod n	N = Crypte^D	Clair = N mod n
0	0	0	0	0
1	1	1	1	1
2	8	8	2 097 152	2
3	27	27	10 460 353 203	3
4	64	31	27 512 614 111	4
5	125	26	8 031 810 176	5
6	216	18	6 122 20 032	6
7	343	13	62 748 517	7
8	512	17	4 103 38 673	8
9	729	3	2 187	9
10	1 000	10	10 000 000	10

© Dunod – La photocopie non autorisée est un délit

Clair	N = Clair^C	Crypte = N mod n	N = Crypte^D	Clair = N mod n
11	1 331	11	194 87 171	11
12	1 728	12	35 831 808	12
13	2 197	19	893 871 739	13
14	2 744	5	78 125	14
15	3 375	9	4 782 969	15
16	4 096	4	16 384	16
17	4 913	29	17 249 876 309	17
18	5 832	24	4 586 471 424	18
19	6 859	28	13 492 928 512	19
20	8 000	14	105 413 504	20
21	9 261	21	180 108 8541	21
22	10 648	22	2 494 357 888	22
23	12 167	23	3 404 825 447	23
24	13 824	30	21 870 000 000	24
25	15 625	16	268 435 456	25
26	17 576	20	1 280 000 000	26
27	19 683	15	170 859 375	27
28	21 952	7	823 543	28
29	24 389	2	128	29
30	27 000	6	279 936	30
31	297 918	25	6 103 515 625	31

Figure 20.83 Table de codage (C = 3, D = 7).

d) Crypte du mot « MODEM »

Clair	M		O			D			E			M	
Hex (8 bits)	4D		4F			44			45			4D	
Binaire 8 bits	01001	101	01	00111	1	0100	0100	0	10001	01		010	01101
Blocs de 5 bits	01001	101	01	00111	1	0100	0100	0	10001	01		010	01101
Clair Décimal	9	21		7	20		8		17	10		13	
Crypte Décimal	3	21		23	14		17		27	10		19	
Blocs de 5 bits	00011	10101		10111	01110		10001		11011	01010		10011	
Binaire 8 bits	00011	101	01	10111	0	11110	1000	1	11011	01		010	10011
Décimal	29		110			232			237			83	
Hex (8 bits)	1D		6E			E8			ED			53	

Figure 20.84 Chiffrement du mot « MODEM ».

Soit le clair : 0x4D, 0x4F, 0x44, 0x45, 0x4D
et le cryptogramme : 0x1D, 0x6E, 0xE8, 0xED, 0x53.

17.6 Système de Diffie-Hellman

Compte tenu des données communes (G = 3, N = 32) et des tirages d'Alice (A = 5) et de Bob (B = 7). Le graphique de la figure 20.85 illustre la méthode de calcul.

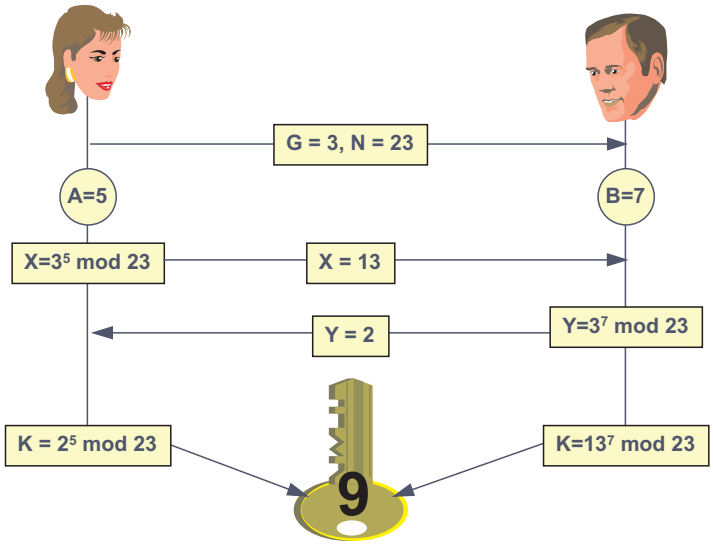


Figure 20.85 Calcul de la clé de session.

CHAPITRE 18

18.1 Analyse de la trace

La figure 20.86 rappelle la structure de la trame Ethernet. Nous n'allons nous intéresser qu'aux champs significatifs.

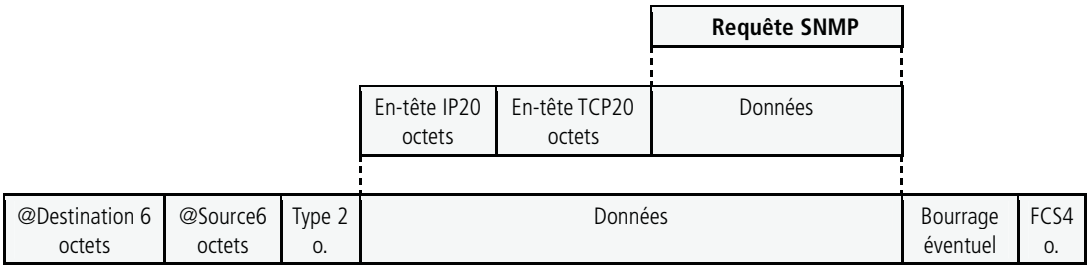


Figure 20.86 Structure de la trame Ethernet.

Décodage de l'en-tête MAC

```
0000: 00 A0 24 BD 75 DB|08 00 02 05 2D FE|08 00
```

Les délimiteurs verticaux marquent les différents champs. Ne retenons que le champ protocole (valeur en gras) qui nous indique bien que le protocole supérieur est IP du DoD (type de protocole 0x08 00).

© Dunod – La photocopie non autorisée est un délit

Décodage de l'en-tête TCP/IP

```
0000:                                              45 00                E.
0010: 00 52 3C EF 00 00 1C 06 A4 FF 80 00 64 00 D0 80  .`<.........d...
0020: 08 29|0A CF 00 A1 47 A8 BA 20 01 A3 96 14 50 18  .)...+G.. ....P.
0030: 20 00 72 D4 00 00
```

L'en-tête IP est en italique, le protocole correspond bien à IP V4 et la longueur d'en-tête est standard (premier octet 45).

Le seul élément intéressant de l'en-tête TCP est le port source (valeur en gras) qui correspond au port 161 (0x 00 A1), c'est-à-dire le port SNMP pour les PDU GetRequest, GetNextRequest et GetResponse.

Décodage du champ données

```
0030:                   30 28 02 01 00 04 06 70 75 62   .r...0c.....pub
0040: 6C 69 63 A0 1B 02 04 03 05 52 AE 02 01 00 02 01  lic.............
0050: 00 30 0D 30 0B 06 07 2B 06 01 02 01 01 03 05 00  .0.0...+........
```

Compte tenu de l'apparente complexité des PDU SNMP, due à la succession de structures, nous avons tenté, dans la représentation ci-dessous, de matérialiser cette imbrication (figure 20.87).

```
30 28
 | 02 01 00
 | 04 06 70 75 62 6C 69 63
 | A0 1B
 |   | 02 04 03 05 52 AE
 |   | 02 01 00
 |   | 02 01 00
 |   | 30 0D
 |   |   | 30 0B
 |   |   |   | 06 07 2B 06 01 02 01 01 03
 |   |   |   | 05 00
```

Figure 20.87 Structure de la PDU SNMP.

Champ	Commentaire
30 28	Le premier octet indique le type 0x30 soit 0011 0000B, il s'agit d'un type de la famille universal, (les deux premiers bits à zéro) construit (3ème bit à 1) et type séquence (1 000). La longueur de la séquence étant de 0x28 soit 40D.
02 01 00	Le type suivant est un entier (0x02) de longueur 1. L'octet suivant indique la version de SNMP, la valeur 0 identifie SNPM v1.
04 06 70 75 62 6C 69 63	Le champ suivant est de type string (0x04) de longueur 6. Il s'agit du champ commity, correspondant au mot de passe : *public*. Les champs suivants contiennent les données de la PDU.

Champ	Commentaire
A0 1B	Le premier champ indique le type et la longueur totale. Le type 0xA0 ou 1010 000B indique qu'il s'agit d'un type dépendant du contexte (10) construit (bit 3 à 1), la valeur 0 des autres éléments binaires identifie la PDU GetRequest. La longueur totale de cette dernière étant de 27 octets (0x1B).
02 04 03 05 52 AE	Ce champ contient le numéro d'identification de la demande. Le type est entier (0x02) de longueur 4 et le contenu 0x03, 0x05, 0x52, 0xAE. La réponse à cette demande contiendra le même identifiant.
02 01 00	Le champ Error_Status est à zéro (ce champ est toujours à zéro dans une PDU de type Get. Type entier 0x02, de longueur 1 (0x01) et de valeur 0 (0x00).
02 01 00	Ce champ est de structure identique au précédent, il s'agit du champ Error_Index, toujours à 0 dans une PDU Get.
30 0D	La valeur 0x30 annonce une nouvelle séquence (universal, construit) de longueur 0x0D soit 13.
30 0B	Le premier champ de cette séquence est lui-même une séquence de longueur 0x0B soit 12.
06 07 2B 06 01 02 01 01 03	Le type de cette séquence est 0x06, c'est un type universal il s'agit du type ID (OID) identifiant l'objet interrogé par la PDU. La longueur de l'OID est de 7. La valeur 0x2B (43D) représente les deux premiers entiers de l'OID selon un codage particulier (A 40 + B) soit 1 40 + 3, l'objet est donc identifié dans l'arbre de nommage par le chemin : 1.3.6.1.2.1.1.3, il s'agit de l'OID de sysUpTime.
05 00	La valeur 0x05 indique le type NIL (NULL). Ce champ indique la fin de la description et des valeurs relatives à l'objet précédemment identifié. Ici, puisqu'il s'agit du PDU de type Get, les champs valeurs sont absents.

18.2 SNMP et charge du réseau

Le nombre de sollicitations est de 100 toutes les 10 s, ce qui correspond à 10 sollicitations par seconde. Dans ces conditions, le volume à transférer est de :

$$(100 \times 8) \times 10 = 8\,000 \text{ bit/s}$$

Ce qui correspond pour une ligne à 64 kbit/s à 12,5 % de ses capacités de transfert. Le protocole SNMP est un protocole « bavard ». L'administration de sites locaux à distance est limitée. Il convient de sélectionner avec la plus grande attention les objets gérés et d'augmenter au maximum la période de polling.

CHAPITRE 19

19.1 Service de vidéotex

La résolution d'un tel problème est simple, il faut d'abord déterminer le trafic à écouler, puis à l'aide de l'abaque définir le nombre de lignes utiles.

© Dunod – La photocopie non autorisée est un délit

Nombre de circuits virtuels

a) Trafic à écouler : $E = NT/3\,600 = 600 \times 2 \times 60/3\,600 = 20$ E.

b) Nombre de lignes pour une qualité de service meilleure que 1 %.

La lecture de l'abaque (figure 20.88, repère ①) donne directement 30 circuits.

Nombre de demandes satisfaites

Nombre de demandes de connexion pour un taux de refus de 2 %

La lecture de l'abaque (figure 20.88, repère ②) indique que pour 30 circuits et un taux de refus de 2 % un trafic écoulé est de 22 E soit un nombre de demande de connexions de

$E = NT/3\,600$ soit $N = 3\,600\,E/T = 3\,600 \times 22/2 \times 60 = 660$ connexions.

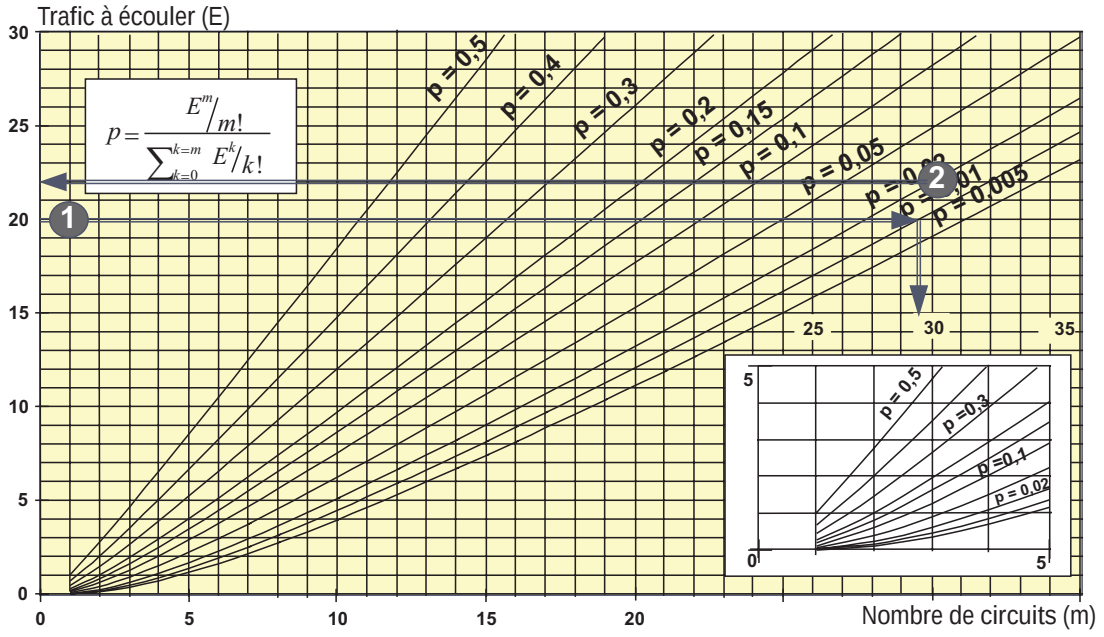


Figure 20.88 Abaque d'Erlang à refus.

19.2 Informatisation d'un magasin

Détermination du nombre de terminaux de caisse

En partant du temps d'attente (t_a) devant les caisses (10 mn) on déterminera la charge maximale supportable (ρ). De cette charge, compte tenu du temps d'encaissement (temps de service ou t_s) on définira le nombre de clients traités par un terminal de caisse.

$$t_a = \frac{\rho}{1-\rho} t_s \quad \text{on déduit} \quad \rho = \frac{t_a}{t_a + t_s} = \frac{10}{10+3} = 0{,}76$$

Une charge maximale de 0,76 correspond à un taux d'arrivée devant le terminal de :

$$\rho = \lambda t_s \quad \text{on déduit} \quad \lambda = \frac{\rho}{t_s} = \frac{0{,}76 \cdot 60}{3} = 15 \text{ clients/heure}$$

Le nombre de clients dans la file sera :

$$N = \lambda t_a = \frac{15 \cdot 10}{60} = 3 \text{ clients}$$

Ce qui répond au cahier des charges, dans ces conditions, il est nécessaire de disposer de 4 terminaux de caisse pour écouler les 60 clients/heure.

Nombre de terminaux au point d'enlèvement

Les terminaux « point d'enlèvement » doivent être accessibles dans 80 % des cas, c'est-à-dire qu'un magasinier ne doit pas se voir refuser l'accès au terminal dans plus de 20 % des cas. Le nombre de terminaux se définit alors à partir des courbes d'Erlang (abaque à refus). Sachant qu'une consultation mobilise le terminal pendant une minute et que 60 clients se présentent dans l'heure, le trafic à écouler est de :

$$E = \frac{Nt}{60} = \frac{60 \cdot 1}{60} = 1 \text{ E}$$

La lecture de l'abaque indique 2 terminaux.

Nombre de terminaux de point de vente

Le raisonnement est identique. Compte tenu qu'il y a 100 consultations de une minute et 60 prises de commande de 3 minutes, le trafic à écouler est de :

$$E = \frac{NT}{60} = \frac{100 \cdot 1 + 60 \cdot 3}{60} = 4{,}66E$$

La lecture de l'abaque, pour un taux de refus de 5 %, donne 8 terminaux.

Le nombre de terminaux à installer est donc de :

Terminaux	Vente	Caisse	Enlèvement	Comptable
Nombre	8	4	2	2

Figure 20.89 Nombre de terminaux.

Temps de réponse

Le temps de réponse exprime le temps d'attente de l'opérateur entre le moment où il valide une requête et celui où la réponse est affichée. La figure 20.90 matérialise les composantes de ce temps.

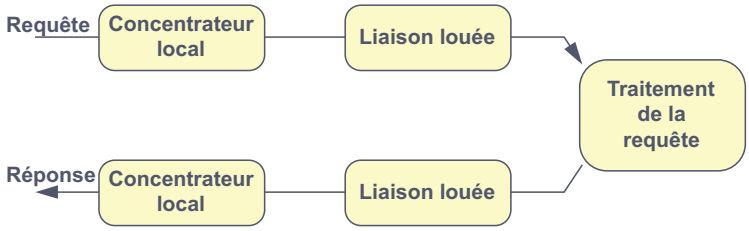


Figure 20.90 Définition du temps de réponse.

© Dunod – La photocopie non autorisée est un délit

Le temps de transport des données sera déterminé à partir de la transaction moyenne. Rappelons, qu'il a 100 transactions/heure point de vente, 60 transactions/heure caisse et enlèvement et 40 transactions/jour (soit 5 transactions/heure) pour les terminaux de comptabilité.

La transaction moyenne doit être définie dans le sens Host/Succursale (L_{HS}) et dans le sens Succursale/Host (L_{SH}), la longueur moyenne sera multipliée par 1,2 pour tenir compte des données de service :

$$L_{HS} = \frac{\Sigma \lambda L}{\Sigma L} = \frac{100 \cdot 800 + 60 \cdot 600 + 60 \cdot 500 + 5 \cdot 800}{100 + 60 + 60 + 5} \cdot 1{,}2 = 800 \text{ octets}$$

$$L_{SH} = \frac{\Sigma \lambda L}{\Sigma L} = \frac{100 \cdot 20 + 60 \cdot 100 + 60 \cdot 20 + 5 \cdot 200}{100 + 60 + 60 + 5} \cdot 1{,}2 = 54{,}4 \text{ octets}$$

Nombre de transactions ou taux d'arrivée :

$$\lambda = \sum \lambda = 100 + 60 + 60 + 5 = 225 \text{ transactions/heure} \quad \text{soit} \quad 0{,}0625 \text{ transaction/seconde}$$

Temps de réponse du concentrateur local (t_{rc}), considéré comme le temps de transfert des données du concentrateur aux terminaux (requête et réponse) :

$$t_{rc} = \frac{L_{HS}}{D_c - \lambda L_{HS}} + \frac{L_{SH}}{D_c - \lambda L_{SH}}$$

$$= \frac{800 \cdot 8}{9\,600 - 0{,}0625 \cdot 800 \cdot 8} + \frac{54{,}4 \cdot 8}{9\,600 - 0{,}0625 \cdot 54{,}4 \cdot 8} = 0{,}74 \text{ s}$$

Temps de réponse de la liaison louée (t_{rt}) :

$$t_{rt} = \frac{L_{Hs}}{D_t - \lambda L_{HS}} + \frac{L_{SH}}{D_t - \lambda L_{SH}}$$

$$= \frac{800 \cdot 8}{64\,000 - 0{,}0625 \cdot 800 \cdot 8} + \frac{54{,}4 \cdot 8}{64\,000 - 0{,}0625 \cdot 54{,}4 \cdot 8} = 0{,}10 \text{ s}$$

Temps de réponse de la transaction :

$$Tr = t_{rc} + t_{rl} + \text{temps de traitement de la requête} = 0{,}74 + 0{,}1 + 0{,}2 = 1{,}04 \text{ s}$$

Nota : rappelons que lorsque le système est peu chargé, ce qui est fréquemment le cas dans les systèmes conversationnels, on peut admettre plus simplement :

$$Tr = \frac{L}{D}$$

19.3 Réalisation d'un réseau privé d'entreprise

a) Graphe du réseau sans contrainte

Matrice des coûts (Kruskal)

La première étape consiste à établir la matrice des coûts, les liens ayant tous un débit identique, cette matrice ne tiendra compte que des distances intersites (figure 20.91).

	Amiens	Lille	Metz	Nancy	Strasbourg	Rennes	Nantes	La Rochelle	Bordeaux	Toulouse	Clermont	Dijon	Lyon	Marseille	Nice
Paris	115	203	283	282	400	310	344	400	500	590	348	264	393	662	687
Amiens		98	296	313	424	353	412	489	603	703	462	351	497	771	786
Lille			283	313	410	444	508	587	699	792	540	396	557	835	834
Metz				47	130	591	613	642	700	713	438	217	386	650	607
Nancy					118	586	600	620	670	674	400	175	341	603	561
Strasbourg						702	713	725	761	738	472	247	384	617	544
Rennes							100	221	373	557	446	512	561	767	849
Nantes								122	275	466	391	499	517	697	792
La Rochelle									154	352	332	491	467	607	718
Bordeaux										213	306	514	437	507	639
Toulouse											275	500	361	320	470
Clermont												228	137	331	404
Dijon													174	449	439
Lyon														278	300
Marseille															160

Figure 20.91 Matrice des coûts.

Liste ordonnée des liens

Ordre	Lien	Distance	Ordre	Lien	Distance
1	Metz Nancy	47	61	Amiens Clermont	462
2	Amiens Lille	98	62	Nantes Toulouse	466
3	Rennes Nantes	100	63	La Rochelle Lyon	467
4	Paris Amiens	115	64	Toulouse Nice	470
5	Nancy Strasbourg	118	64	Strasbourg Clermont	472
6	Nantes La Rochelle	122	66	Amiens La Rochelle	489
7	Metz Strasbourg	130	67	La Rochelle Dijon	491
8	Clermont Lyon	137	68	Amiens Lyon	497
9	La Rochelle Bordeaux	154	69	Nantes Dijon	499
10	Marseille Nice	160	70	Paris Bordeaux	500

© Dunod – La photocopie non autorisée est un délit

Ordre	Lien	Distance	Ordre	Lien	Distance
11	Dijon Lyon	174	71	Toulouse Dijon	500
12	Nancy Dijon	175	72	Bordeaux Marseille	507
13	Paris Lille	203	73	Lille Nantes	508
14	Bordeaux Toulouse	213	74	Rennes Dijon	512
15	Metz Dijon	217	75	Bordeaux Dijon	514
16	Rennes La Rochelle	221	76	Nantes Lyon	517
17	Clermont Dijon	228	77	Lille Clermont	540
18	Strasbourg Dijon	247	78	Strasbourg Nice	544
19	Paris Dijon	264	79	Lille Lyon	557
20	Nantes Bordeaux	275	80	Rennes Toulouse	557
21	Toulouse Clermont	275	81	Nancy Nice	561
22	Lyon Marseille	278	82	Rennes Lyon	561
23	Paris Nancy	282	83	Nancy Rennes	586
24	Paris Metz	283	84	Lille La Rochelle	587
25	Lille Metz	283	85	Paris Toulouse	590
26	Amiens Metz	296	86	Metz Rennes	591
27	Lyon Nice	300	87	Nancy Nantes	600
28	Bordeaux Clermont	306	88	Amiens Bordeaux	603
29	Paris Rennes	310	89	Nancy Marseille	603
30	Amiens Nancy	313	90	Metz Nice	607
31	Lille Nancy	313	91	La Rochelle Marseille	607
32	Toulouse Marseille	320	92	Metz Nantes	613
33	Clermont Marseille	331	93	Strasbourg Marseille	617
34	La Rochelle Clermont	332	94	Nancy La Rochelle	620
35	Nancy Lyon	341	95	Bordeaux Nice	639
36	Paris Nantes	344	96	Metz La Rochelle	642
37	Paris Clermont	348	97	Metz Marseille	650
38	Amiens Dijon	351	98	Paris Marseille	662
39	La Rochelle Toulouse	352	99	Nancy Bordeaux	670
40	Amiens Rennes	353	100	Nancy Toulouse	674
41	Toulouse Lyon	361	101	Paris Nice	687
42	Rennes Bordeaux	373	102	Nantes Marseille	697
43	Strasbourg Lyon	384	103	Lille Bordeaux	699
44	Metz Lyon	386	104	Metz Bordeaux	700
45	Nantes Clermont	391	105	Strasbourg Rennes	702
46	Paris Lyon	393	106	Amiens Toulouse	703
47	Lille Dijon	396	107	Metz Toulouse	713

Ordre	Lien	Distance	Ordre	Lien	Distance
48	Paris Strasbourg	400	108	Strasbourg Nantes	713
49	Paris La Rochelle	400	109	La Rochelle Nice	718
50	Nancy Clermont	400	110	Strasbourg La Rochelle	725
51	Clermont Nice	404	111	Strasbourg Toulouse	738
52	Lille Strasbourg	410	112	Strasbourg Bordeaux	761
53	Amiens Nantes	412	113	Rennes Marseille	767
54	Amiens Strasbourg	424	114	Amiens Marseille	771
55	Bordeaux Lyon	437	115	Amiens Nice	786
56	Metz Clermont	438	116	Lille Toulouse	792
57	Dijon Nice	439	117	Nantes Nice	792
58	Lille Rennes	444	118	Lille Nice	834
59	Rennes Clermont	446	119	Lille Marseille	835
60	Dijon Marseille	449	120	Rennes Nice	849

Figure 20.92 Liste ordonnée des coûts.

Constitution du réseau de premier niveau (sans contrainte)

Le tableau de la figure 20.93 synthétise la démarche permettant de retenir les liens constituant le réseau de premier niveau. La figure 20.94 illustre ce réseau. Tandis que le tableau de la figure 20.95 indique le coût de ce réseau.

Ordre	Lien	Distance	Ordre	Lien	Distance
1	Metz Nancy	47	12	Nancy Dijon	175
2	Amiens Lille	98	13	Paris Lille	Boucle
3	Rennes Nantes	100	14	Bordeaux Toulouse	213
4	Paris Amiens	115	15	Metz Dijon	Boucle
5	Nancy Strasbourg	118	16	Rennes La Rochelle	Boucle
6	Nantes La Rochelle	122	17	Clermont Dijon	Boucle
7	Metz Strasbourg	Boucle	18	Strasbourg Dijon	Boucle
8	Clermont Lyon	137	19	Paris Dijon	264
9	La Rochelle Bordeaux	154	20	Nantes Bordeaux	Boucle
10	Marseille Nice	160	21	Toulouse Clermont	275
11	Dijon Lyon	174	22	Lyon Marseille	278

Figure 20.93 Détermination des liens du réseau de premier niveau

© Dunod – La photocopie non autorisée est un délit

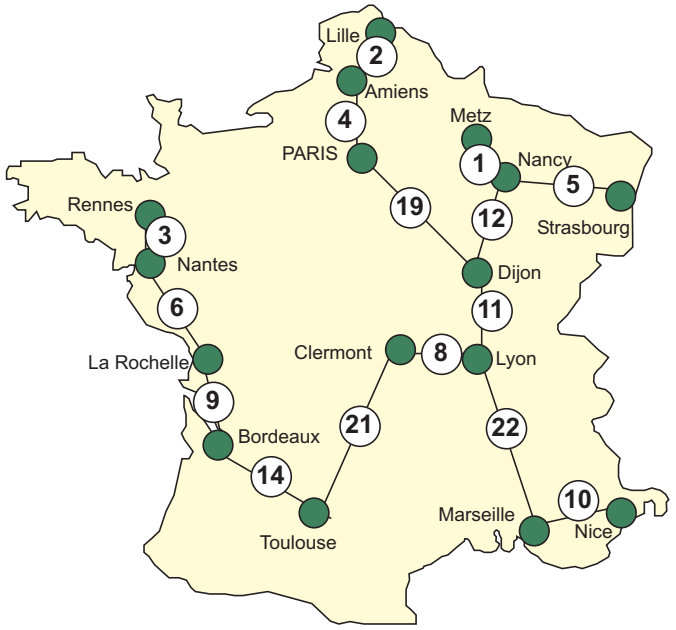


Figure 20.94 Topologie du réseau de premier niveau

Ordre	Lien	Distance
1	Metz Nancy	47
2	Amiens Lille	98
3	Rennes Nantes	100
4	Paris Amiens	115
5	Nancy Strasbourg	118
6	Nantes La Rochelle	122
8	Clermont Lyon	137
9	La Rochelle Bordeaux	154
10	Marseille Nice	160
11	Dijon Lyon	174
12	Nancy Dijon	175
14	Bordeaux Toulouse	213
19	Paris Dijon	264
21	Toulouse Clermont	275
22	Lyon Marseille	278
Coût total (km)		**2 430**

Figure 20.95 Détermination du coût du réseau

b) Constitution du réseau sous contrainte

La démarche est identique, si ce n'est que l'on refuse les liens ne respectant pas les contraintes imposées. La contrainte de débit impose un maximum de trois sites sur un lien concentré (deux noeuds et le site lui-même) et celle du nombre de bonds n'admets qu'un seul site derrière un noeud (figure 20.96). Remarquons que du fait de la sporadicité des transferts, le débit réel offert à chaque site pourra atteindre, par instant, les 64 000 bits/s de débit nominal de la liaison.

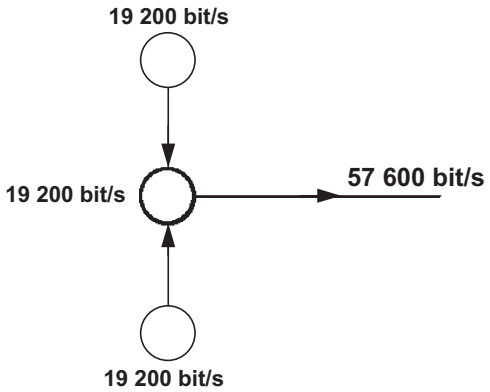


Figure 20.96 Concentration des noeuds.

En respectant les contraintes énoncées, on définit le réseau dont la topologie est représentée figure 20.97.

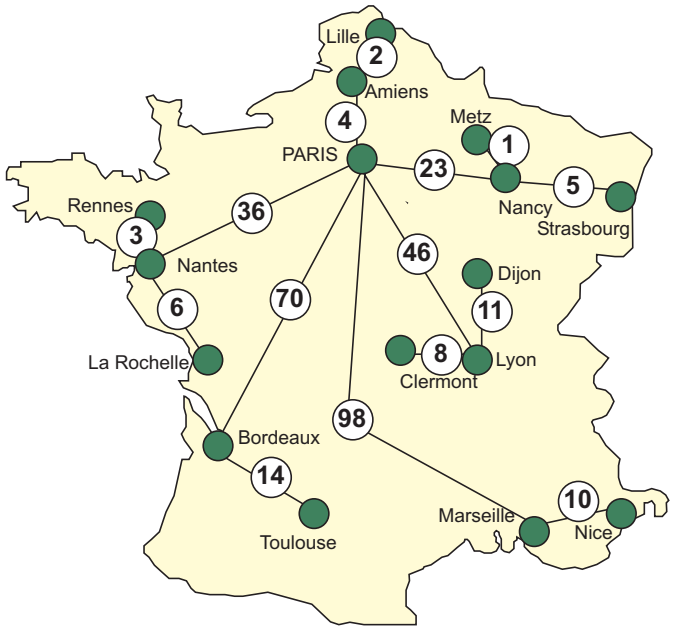


Figure 20.97 Topologie du réseau sous contrainte.

© Dunod – La photocopie non autorisée est un délit

Coût du réseau sous contrainte :

Ordre	Lien	Distance
1	Metz Nancy	47
2	Amiens Lille	98
3	Rennes Nantes	100
4	Paris Amiens	115
5	Nancy Strasbourg	118
6	Nantes La Rochelle	122
8	Clermont Lyon	137
10	Marseille Nice	160
11	Dijon Lyon	174
14	Bordeaux Toulouse	213
23	Paris Nancy	282
36	Paris Nantes	344
46	Paris Lyon	393
70	Paris Bordeaux	500
98	Paris Marseille	662
Coût total (km)		**3 465**

Figure 20.98 Coûts du réseau sous contrainte.

19.4 Caractéristique mémoire d'un routeur

Taux d'arrivée des paquets (λ)

Le taux d'arrivée des paquets se détermine en appliquant le principe de la superposition des flux, soit :

$$\lambda = 2 \times\ 4 + 2 \times\ 2 + 3 \times\ 6 + 5 \times\ 5 = 55 \text{ paquets/seconde}$$

Taux de service (μ)

Le taux de service représente le nombre de paquets traités par seconde. Il est donné par la relation :

$\mu = 1/\text{ts}$ où ts représente le temps de service soit,

$\text{ts} = (128 \times 8/64\,000) = 16\ \text{ms}$

$\mu = 1/1610^{-3} = 62{,}5$ paquets/seconde

Charge du système (ρ)

La charge du système ou intensité de trafic est le rapport entre la charge soumise et la charge admissible :

$$\rho = 55/62{,}5 = 0{,}88$$

Notons que le système est stable ($\rho < 1$), mais proche de la saturation.

Nombre de paquets dans le routeur (N)

Le nombre de paquets dans le routeur est donné par la relation :

$$\mathrm{N} = \rho/(1-\rho) \quad \text{soit} \quad \mathrm{N} = \rho/(1-\rho) = 0{,}88/(1-0{,}88) = 7{,}3 \text{ paquets}$$

Temps moyen d'attente (ta)

Le temps moyen d'attente correspond au produit du nombre de paquets dans le routeur par le temps de traitement d'un paquet (temps de service) soit :

$$\mathrm{ta} = \mathrm{N} \times \mathrm{ts} = 7{,}3 \times [(128 \times 8)/64\,000] = 7{,}3 \times 0{,}016 = 0{,}1168 \text{ seconde}$$

Nombre de paquets dans la file d'attente (Paquets en attente, Na)

$$\mathrm{Na} = \lambda \times \mathrm{ta} = 55 \times 0{,}1168 = 6{,}424 \text{ paquets}$$

Temps de réponse ou temps de queue (tq)

$$\mathrm{tq} = \mu/\lambda = 7{,}3/55 = 0{,}1327 \text{ s}$$

Taille du buffer (T)

$$\mathrm{T} = \text{Nombre d'items en attente} \times \text{taille d'un item} = 6{,}424 \times 128 = 822 \text{ octets}$$

On retiendra une taille buffer de 1 ko soit une contenance de 8 paquets, la file d'attente est donc du type M/M/1/8.

Probabilité de perte d'un item

Nombre moyen de paquets dans le système : 7,3 paquets.

si $\rho \neq 1$

$$p_n = \frac{\rho^n(1-\rho)}{1-\rho^{K+1}} = \frac{0{,}88^{7{,}3}(1-0{,}88)}{1-0{,}88^{8+1}} = 0{,}075$$

Notons que pour une charge de 50 %, la probabilité de perte serait encore de 2 %, c'est là que réside la difficulté du dimensionnement des mémoires tampons dans les éléments actifs.

19.5 Temps de transit dans un réseau

La méthode consiste à considérer le réseau comme une seule file d'attente et d'appliquer la relation de Little pour déterminer le temps de transit. Pour cela, il convient, à partir du trafic écoulé par chaque nœud, de déterminer le nombre de paquets en transit dans le réseau et d'appliquer ensuite la relation de Little.

© Dunod – La photocopie non autorisée est un délit

Lien	Proportion du trafic écoulé
N1-N2	75 %
N2-N4	50 %
N3-N5	25 %

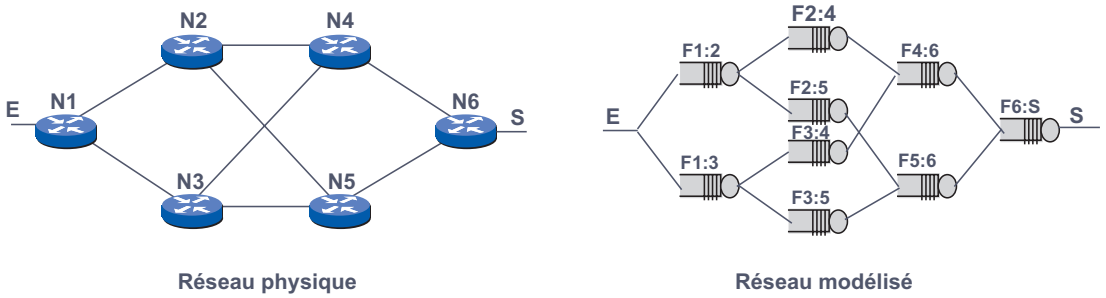


Figure 20.99 Réseau modélisé.

Rappelons les conditions :

Longueur moyenne d'un paquet 128 octets

Débit des liens 64 kbit/s

Taux d'arrivée en E : $\lambda = 30$ paquets/s

Temps de service : ts = 128 × 8/64 000 = 16 ms

Taux de service : $\mu = 1/ts = 1/16\ 10^{-3} = 62{,}5$ paquet/s

D'où le tableau de synthèse suivant :

File	Trafic %	Taux d'arrivée λ	Charge $\rho = \lambda / \mu$	Nb items dans le nœud $\mu = \rho / (1-\rho)$
F1:2	0,75	22,5	0,36	0,5625
F1:3	0,25	7,5	0,12	0,1363
F2:4	0,375	11,25	0,18	0,2195
F2:5	0,375	11,25	0,18	0,2195
F3:4	0,1875	5,625	0,09	0,098
F3:5	0,0625	1,875	0,03	0,0309
F4:6	0,5625	16,875	0,27	0,3698
F5:6	0,4375	13,125	0,21	0,2658
F6:S	1	30	0,48	0,9230
Nombre de paquets dans le réseau :				2,8253

Figure 20.100 Paquets en transit dans le réseau.

Temps de transit dans le réseau : $N = \lambda \times tq$ soit $tq = N/\lambda = 2{,}8253/30 = 94$ ms.

Annexes

A. DÉFINITIONS

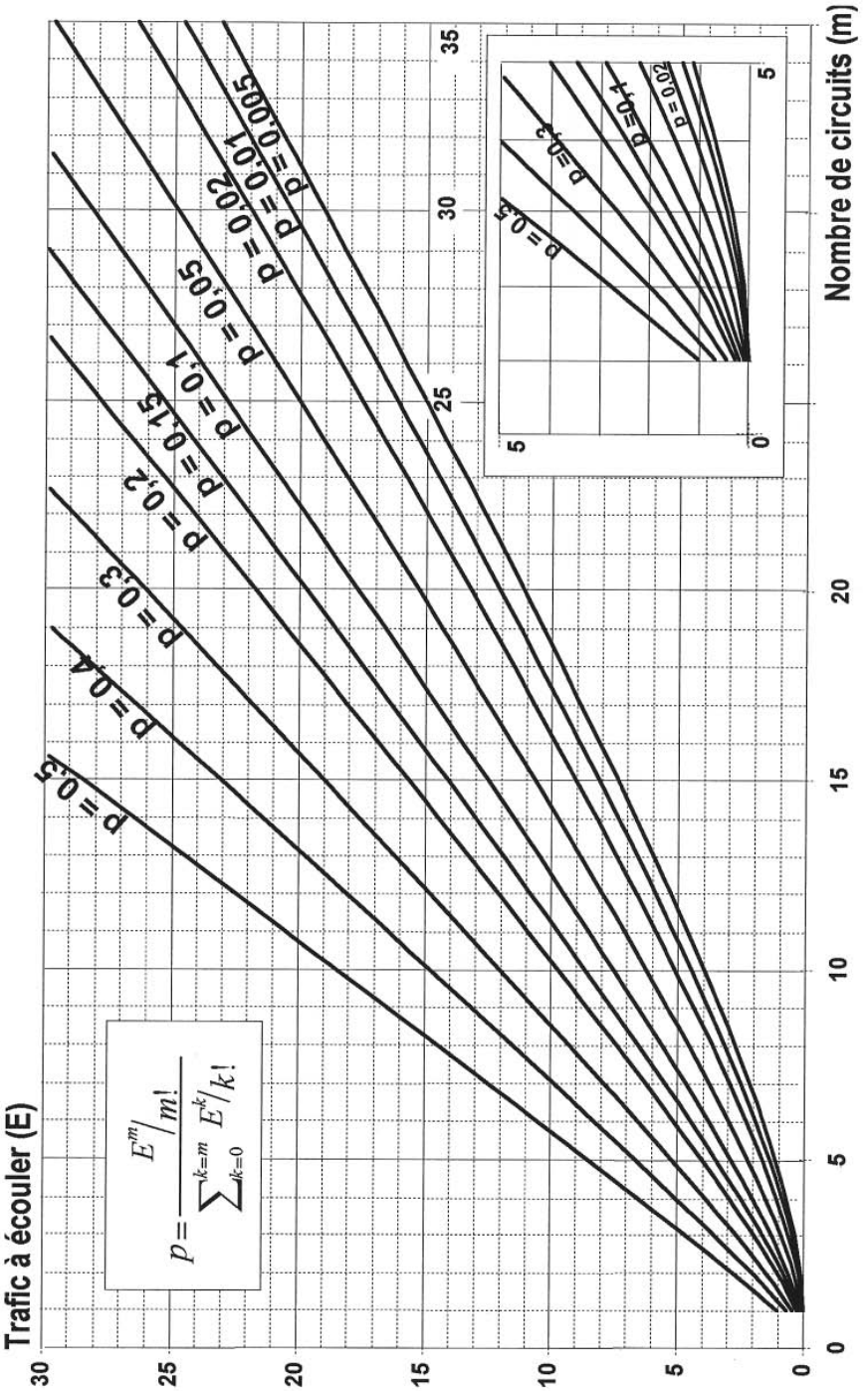
B. ABAQUES D'ERLANG

C. LISTE DES ABRÉVIATIONS ET SIGLES UTILISÉS

A. DÉFINITIONS

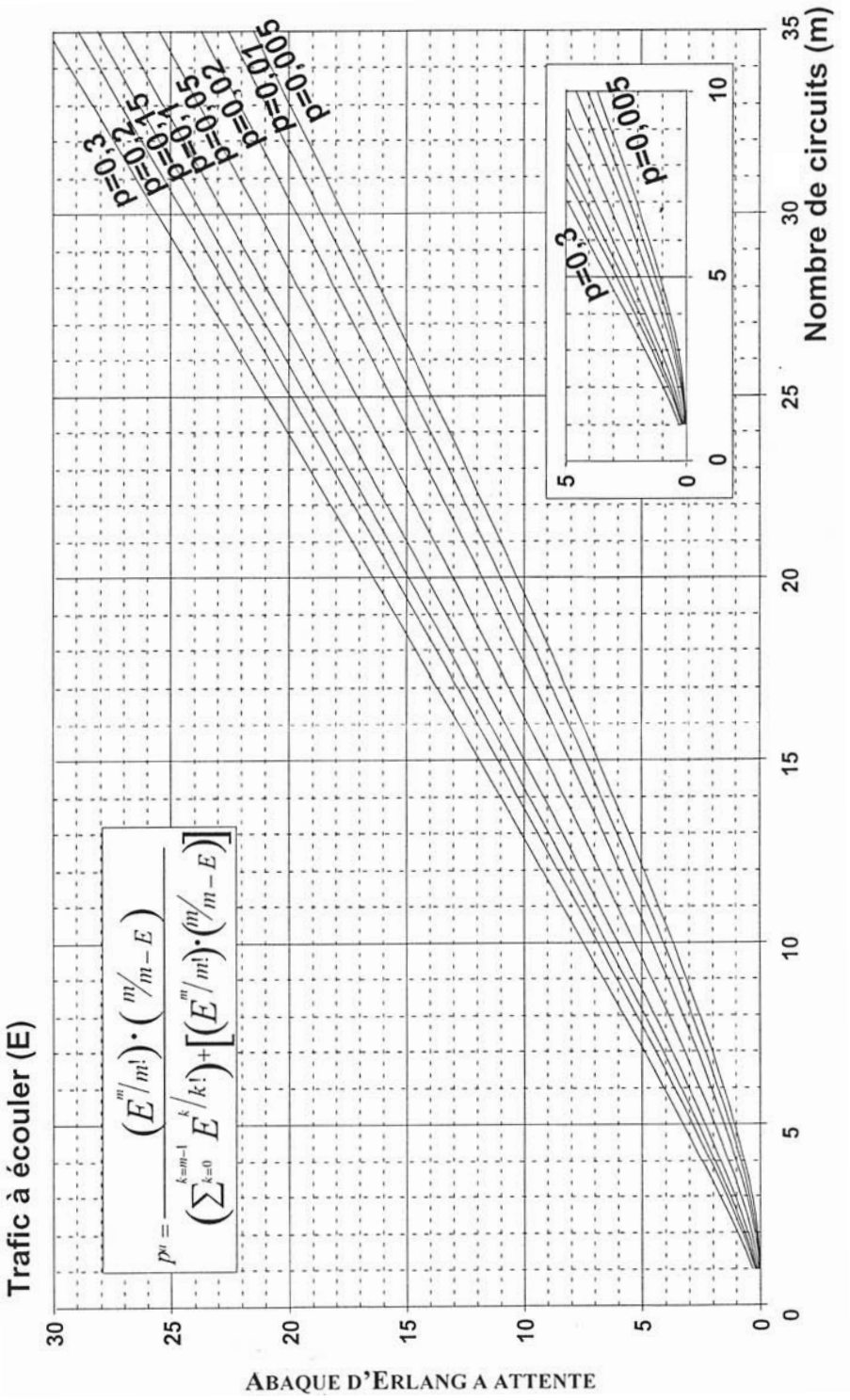
	ASYNCHRONE	SYNCHRONE	ISOCHRONE	PLESIOCHRONE
Trafic ou flux de données	Notion utilisée dans les réseaux FDDI, les données de la classe asynchrone correspondent à un flux auquel n'est attachée aucune contrainte temporelle.	Notion utilisée dans les réseaux FDDI, les données de la classe synchrone correspondent à un flux auquel est attachée une légère contrainte temporelle (réservation de bande passante).	Données ayant une contrainte temporelle forte en relation non seulement avec le temps de transfert mais aussi sur le rythme de délivrance des informations. Exemple : la voix.	
Transmission	Transmission en mode caractères ou blocs, chaque caractère comporte un délimiteur de début et de fin (bit de start, bit de stop).	Transmission en mode blocs, chaque bloc comporte un délimiteur de début de bloc et de fin (fanion), les caractères ne sont pas délimités.		
Mode de transfert	Données émises au rythme de la source (mode paquets ou ATM).	Données émises au rythme du réseau (mode circuit ou STM).		
Réseau		Tous les nœuds du réseau ont une même référence temporelle (même horloge). Exemple : Token Ring.		Chaque nœud du réseau à sa propre horloge. Exemple : Ethernet, FDDI.
Terminal	Terminal en mode caractère. Exemple : VT100, Minitel.	Terminal en mode bloc.		

B. ABAQUES D'ERLANG



ABAQUE D'ERLANG A REFUS

© Dunod – La photocopie non autorisée est un délit


Trafic à écouler (E)
Nombre de circuits (m)
p=0,3
p=0,25
p=0,15
p=0,1
p=0,05
p=0,02
p=0,01
p=0,005
p=0,
p=0,3
p=0,005
$P^{(x)} = \frac{\left(E^m/m!\right)\cdot\left(m/m-E\right)}{\left(\sum_{k=0}^{k=m-1} E^k/k!\right)+\left[\left(E^m/m!\right)\cdot\left(m/m-E\right)\right]}$
ABAQUE D'ERLANG A ATTENTE

C. LISTE DES ABRÉVIATIONS ET SIGLES UTILISÉS

AAL *ATM Adaptation Layer*
ABM *Asynchronous Balanced Mode*
ABR *Available Bit Rate*
ACF *Advanced Communication Function*
Ack *Acknowledge*
ACR *Attenuation Crosstalk Ratio*
ADCCP *Advanced Data Communication Control Protocol*
ADPCM *Adaptative Differential Pulse Code Modulation*
ADSL *Asymmetric Data Subscriber Line*
AF *Assured Forwarding*
AFI *Autority Format Identifier*
AFNOR Association Française de NORmalisation
AMRT Accès Multiple à Répartition dans le Temps
ANSI *Americain National Standard Institute*
AP *Application Proccess*
API *Application Program Interface*
ARIS *Aggregate Route-based IP Switching*
ARM *Asynchronous Response Mode*
ARP *Address Resolution Protocol*
ART Autorité de Régulation des Télécommunication
ASCE *Association Control Service Element*
ASCII *Americain Standard Code for Information Interchange*
ASE *Application Service Element*
ASN 1 *Abstract Syntax Notation One*
ASP *Application Service Provider*
ATM *Asynchronous Transfer Mode*
AU *Administrative Unit*
B-ICI-NNI *Broadband Inter-Carrier Interface Network to Network Interface*
B-ISDN *Broadband Integrated Service Digital Network*
BAS *Basic Activity Subset*
Bc *Committed Burst Size*
BCC *Block Check Character*
BCD *Binary Code Decimal*
BCS *Bull Cabling System*
Be *Excess Burst size*
BEB *Binary Exponentiel Backoff*
BECN *Backward Explicit Congestion Notification*
BLR Boucle Locale Radio
BLU Bande Latérale Unique
BNC *Barrel Neck Connector*
BOF *Birth Of a Feature*
BSC *Basic Combined Subset*
BSC *Binary Synchronous Communication*
BSI *British Standard Institute*
BSS *Basic Synchronized Subset*
BUS *Broadcast and Unknown Server*
C/R *Commande/Response*
CAC *Connection Admission Call*
CAP *Carrier Amplitude and Phase modulation*
CAS *Channel Associated Signaling*
CATV Cable TéléVision
CBDS *Connectionless Broadband Data Service*
CBR *Constant Bit Rate*
CCITT Comité Consultatif International pour le Télégraphe et le Téléphone
CCR *Current Cell Rate*
CCRSE *Commitment Concurency and Recovery Service Element*
CCS *Common Channel Signaling*

© Dunod – La photocopie non autorisée est un délit

CDV *Cell Delay Variation*
CEI Commission Electrotechnique Internationale
CELP *Code Excited Linear Prediction*
CER *Cell Error Ratio*
CES *Circuit Emulation Structured*
CI *Congestion Indication*
CIDR *Classless InterDomain Routing*
CIR *Committed Information Rate*
CLLM *Consolited Link Layer Management*
CLNAP *ConnectionLess Network Access Protocol*
CLNIP *Connectionless Network Interface Protocol*
CLNS *ConnectionLess Network Service*
CLP *Cell Loss Priority*
CLR *Cell Loss Ratio*
CLS *ConnectionLess Server*
CMR *Cell Misinsertion Rate*
CNLS *ConnectionLess Oriented Network Service*
CODEC COdeur DECodeur
COF *Connection Oriented Function*
CONS *Connection Oriented Network Service*
CoS *Class of Service*
COS *Comittee Of Standardization*
CPCS *Common Part Convergence Sublayer*
CPI *Common Part Indication*
CRC *Cyclic Redundancy Check*
CS *Convergence Sublayer*
CSI *Convergence Sublayer Information*
CSMA *Carrier Send Multiple Access*
CSR *Cell Switched Router*
CSS *Common Channel Signaling*
CTD *Cell Transfert Delay*
CTI Couplage Téléphonie/Informatique
CV Circuit Virtuel
CVC Circuit Virtuel Commuté
CVP Circuit Virtuel Permanent
DAC *Double Attachment Concentrator*
DARPA *Defence Advanced Projet Adgency USA*
DAS *Double Attachment Station*
DBR *Deterministic Bit Rate*
DCB Décimal Codé Binaire
DCE *Data Circuit Equipment*
DDCMP *Digital Data Communication Message Protocol*
DE *Discard Eligibility*
DECT *Digital Enhanced Cordless Telephone*
DES *Data Encryption Standard*
DF *Do not Fragment*
DHCP *Dynamic Host Configuration Protocol*
DiffServ *Differentiated Services*
DIN *Deutsches Institut für Normung*
DISOSS *Distributed Office Support System*
DIT *Directory Information Tree*
DIX Digital, Intel et Xerox
DLCI *Data Link Connection Identifier*
DM-PDU *Derived MAC PDU*
DMT *Discrete MultiTone*
DMZ *DeMilitarized Zone*
DNIC *Data Network Identification Code*
DNS *Domain Name System*
DoD *Department of Defence*
DPAM *Demand Priority Access Method*
DQDB *Distributed Queue Dual Bus*
DS *Directory Service*
DSA *Distributed System Architecture*
DSAP *Destination Service Access Point*
DSL *Digital Subscriber Line*
DSP *Domain Specific Part*
DTE *Data Terminal Equipment*
DTL *Designated Transit List*
DTMF *Dual Tone Multi Frequency*

DTP *Distributed Transaction Processing*
DWDM *Dense WDM*
E&M *Earth and Mouth*
EA *End Address*
EB *Elasticity buffer*
EBCDIC *Extended Binary Decimal Interchange Code*
EBCI *Explicit Backward Congestion Identifier*
ECMA *European Computer Manufactures Association*
ECN *Explicit Congestion Notification*
ECR *Explicit Cell Rate*
EFCI *Explicit Forward Congestion Identifier*
EFCN *Explicit Forward Congestion Notification*
EIA *Electronic Industries Association*
EIR *Excess Information Rate*
ELAN *Emulated LAN*
EOP *Element of Procedure*
EPD *Early Packet Discard*
ERBdB Emetteur-Récepteur en Bande de Base
ES *End System*
ESI *End System Identifier*
ETCD Equipement Terminal de Circuit de Données
ETR *Early Token Release*
ETTD Equipement Terminal de Traitement de Données
FCS *Fibre Channel Standard*
FCS *Frame Check Sequence*
FDDI *Fiber Distributed Data Interface*
FDM *Frequency Division Multiplexing*
FDSE *Full Duplex Switched Ethernet*
FEC *Forwarding Equivalence Class*
FECN *Forward Explicit Congestion Notification*
FLP *Fast Link Pulse*
FR *Frame Relay* (relais de trames)
FRAD *Frame Relay Access Device*
FSK *Frequency Shift Keying*
FTAM *File Transfer Access and Management*
FTP *File Transfer Protocol*
FTP *Foiled Twisted Pair*
GFA Groupe Fermé d'Abonnés
GFC *Generic Flow Control*
GFU Groupe Fermé d'Utilisateurs
GMPLS *Generalized MPLS*
GPRS *General Packet Radio Services*
GPS *Global Positioning System*
GSM *Global System for Mobile communications*
GSMP *General Switch Management Protocol*
HDBn Haute Densité Binaire d'ordre *n*
HDLC *High Level Data Link Protocol*
HDSL *High data rate DSL*
HEC *Header Error Control*
HEL *Header Extension Length*
HiPPI *High Performance Parallel Interface*
HLPI *Higher Layer Protocol Identifier*
HSTRA *High Speed Token Ring Alliance*
HTML *Hyper Text Markup Language*
HTTP *Hyper Text Transfer Protocol*
IAB *Internet Activities Board*
ICF *Isochronous Convergence Function*
ICMP *Internet Control and error Message Protocol*
ICS *IBM Cabling System*
IDI *Initial Domain Identifier*
IDP *Initial Domain Part*
IEEE *Institue of Electrical and Electronics Enginers*
IFG *InterFrame Gap*
IGRP *Interior Gateway Routing Protocol*
IISP *Interim Inter Switch Protocol*

© Dunod – La photocopie non autorisée est un délit

IKE *Internet Key Exchange*
ILMI *Interim Local Management Interface*
IM-PDU *Initial MAC Protocol Data Unit*
InARP *Inverse ARP*
IntServ *Integrated Services*
IP *Internet Protocol*
IPBX *Internet Protocol private Branch eXchange*
IPsec *IP Security*
IRL *Inter Repeater Link*
IS-IS *Intermediate System to Intermediate System*
ISDN *Integrated Services Digital Network*
ISO *International Standardization Organization*
IT Intervalle de Temps
JPEG *Joint Photographic Experts Group*
JTM *Job Transfer and Manipulation*
LAN *Local Area Network*
LAP *Link Access Protocol*
LASER *Light Amplification by Stimulated Emission of Radiation*
LC *Late_Counter*
LCR *Least Cost Routing*
LDAP *Lightweight Directory Access Protocol*
LDP *Label Distribution Protocol*
LEC *LAN Emulation Client*
LEC-ID *LEC-Identifier*
LECS *LAN Emulation Configuration Server*
LED *Light Emitting Diode*
LER *Label Edge Router*
LES *LAN Emulation Server*
LI *Length Indicator*
LIA Liaison Inter-Automatique
LIS *Logical IP Subnetworking*
LL Liaison Louée
LLC *Logical Link Control*
LMI *Layer Management Interface*
LPDU *Link Protocol Data Unit*
LRC *Longitudinal Redundancy Check*
LS Liaison Spécialisée
LSAP *Link Service Access Point*
LSDU *Link Service Data Unit*
LSP *Label Switched Path*
LSR *Label Switched Router*
LTP *Link Test Pulses*
LU *Logical Unit*
LUNI *LAN emulation User to Network Interface*
LVC Liaison Virtuelle Commutée
LVR Liaison Virtuelle Réservée
MAC *Medium Access Control*
MACF *Multiple Association Control Function*
MAN *Metropolitain Area Network*
MAU *Medium Access Unit*
MBGP MPLS BGP
MBS *Maximum Burst Size*
MCF *MAC Convergence Function*
MCR *Minimum Cell Rate*
MCU *Multipoint Control Unit*
MDI *Medium Dependent Interface*
MHS *Message Handling System*
MIC Modulation par Impulsion et Codage
MII *Medium Independent Interface*
MMF *MultiMode optical Fiber*
MNP *Microcom Networking Protocol*
MOCAM Modem à Carte A Mémoire
MODEM MODulateur DEModulateur
MPEG *Motion Picture Expert Group*
MPLS *MultiProtocol Label Switching*
MPλS *MultiProtocol Lamda Switching*
MPOA *MultiProtocol Over ATM*
MSS *Maximum Segment Size*
MTBF *Mean Time Between Failure*

MTTR *Mean Time To Repair*
MTU *Maximum Transfert Unit*
NBS *National Bureau of Standards*
NCP *Network Control Program*
NEXT *Near End Crosstalk loss*
NHRP *Next Hop Resolution Protocol*
NI *No Increase*
NIC *Network Information Center*
NLPID *Network Level Protocol ID*
NNI *Network Node Interface*
NNI *Network to Network Interface*
NPR *Normal Priority Request*
NRM *Normal Response Mode*
NRZ *Non Return to Zero*
NRZI *No Return to Zero Inverted*
NTI Nœud de Transit International
NTT *Nippon Telephon and Telegraph Corporation*
NUA *Network User Address*
NVL Numéro de Voie Logique
OAM *Operation And Maintenance*
OCR *Optical Character Recogniton*
ODA *Office Document Architecture*
OSI *Open System Interconnection*
OSNS *Open System Network Service*
OSPF *Open Short Path First*
OSTSS *Open System Transport and Session Support*
OUI *Organizational Unit Identifier*
OXC *Optical Cross Connect*
PABX *PrivAte Branch eXchange*
PAD *Packet Assembler Disassembler*
PAF *Pre-Arbitrated Function*
PAVI *Point Accès VIdéotex*
PBX *Private Branch eXchange*
PCI *Protocol Control Information*
PCM *Pulse Code Modulation*
PCR *Peak Cell Rate*
PDH *Plesiochronous Digital Hierarchy*
PDU *Protocol Data Unit*
PE *Provider Edge*
PID *Protocol ID*
PIH *Protocol Identifier Header*
PIN *Personal Identifier Number*
PIN *Positive Intrinsic Negative*
PIU *Path Information Unit*
PL *PAD Length*
PL-OH *Physical Layer Over Head*
PM *Physical Medium*
PMD *Physical Medium Dependent*
PMI *Physical Medium Independent*
PNNI *Private Network to Network Interface*
POH *Path OverHead*
POSI *Promotion conference for OSI*
PPP *Point to Point Protocol*
PSK *Phase Shift Keying*
PTI *Payload Type Identifier*
Pty *Parity Bit*
PU *Physical Unit*
PVC *Permanent Virtual Circuit*
QAF *Queue Arbitrated Function*
QoS *Quality of Service*
QPSX *Queue Packet Dual Bus*
RA *Request Acknowledge*
RARP *Reverse Address Resolution Protocol*
RAS *Registration Admission Session*
RAS *Rivest Shamir Adleman*
RDA *Remote Databade Access*
RFC *Request For Comments*
RIP *Routing Information Protocol*
RLE Réseaux Locaux d'Entreprise
RLE *Run Length Encoding*
RM *Ressource Management*
RNIS Réseau Numérique à Intégration de Service

© Dunod – La photocopie non autorisée est un délit

RNIS-LB RNIS Large Bande
RNR *Receive Not Ready*
RON/TRON RéceptiON et TRansmissiON
ROSE *Remote Operation Service Element*
RR *Receive Ready*
RR *Relative Rate*
RSVP *Ressource ReserVation Protocol*
RTC Réseau Téléphonique Commuté
RTCP *Real Time Control Protocol*
RTP *Real Time Transport Protocol*
RTS *Real Time Stamp*
RTSE *Reliable Transfer Service Element*
RTSP *Real Time Stream control Protocol*
SAAL *Signaling AAL*
SABM *Set Asynchronous Balanced Mode*
SAC *Single Attachment Concentrator*
SACF *Simple Association Control Function*
SALL *Signaling AAL*
SAO *Simple Application Objet*
SAP *Service Access Point*
SAR *Segmentation And Reassembly*
SAS *Single Attachment Station*
SBR *Statistical Bit Rate*
SCR *Sustainable Cell Rate*
SDA Sélection Directe à l'Arrivée
SDH *Synchronous Digital Hierarchy*
SDLC *Synchronous Data Link Control*
SDU *Service Data Unit*
SECAM SEquentiel Couleur A Mémoire
SEL *SELector field.*
SF *SuperFrame*
SFD *Start Frame Delimitor*
SHTTP *Secure HTTP*
SIM *Subscriber Identification Module*
SIP *Session Initiation Protocol*
SLA *Service Level Agreement*
SLIP *Serie Line Internet Protocol*
SMF *Single Mode optical Fiber*
SMON *Switched RMON*
SN *Sequence Number*
SNA *System Network Architecture*
SNACP *SubNetwork Access Protocol*
SNAP *SubNetwork Access Protocol*
SNC *Sequence Number Counter*
SNDCP *SubNetwork Dependant Convergence Protocol*
SNICP *SubNetwork Independant Convergence Protocol*
SNP *Sequence Number Protection*
SNPA *SubNetwork Point of Attachment*
SOH *Section OverHead*
SONET *Synchronous Optical NETwork*
SPAG *Standard Promotion and Application Group*
SSAP *Source Service Access Point*
SSCS *Service Specific Convergence Sublayer*
SSCS *Service Specific Convergence Sublayer*
SSL *Secure Socket Layer*
STM *Synchronous Transfer Mode*
STP *Shielded Twisted Pairs*
SVC *Switched Virtual Circuit*
Tc *Committed rate measurement interval*
TC Transmission Convergence
TCCA *Time Critical Communication Architecture*
TCP *Transmission Control Protocol*
TDM *Time Division Multiplexing*
TDP *Tag Distribution Protocol*
THT *Token Holding Timer*
TINA *Telecommunication Information Networking Architecture*
TNR Terminaison Numérique de Réseau
TP_IDL *Twisted Pair Idle Signal*
TPDDI *Twisted Pair Distributed Data Interface*

TRT *Token Rotation Timer*
TTI Taux de Transfert des Informations
TTL *Time To Live*
TTRT *Target Token Rotation Time*
UBR *Unspeciefied Bit Rate*
UCR *User Cell Rate*
UDP *User Datagram Protocol*
UE *User Element*
UI *Unnumbered Information*
UIT Union Internationale des Télécommunications
UMTS *Universal Mobile Telecommunication System*
UNI *User to Network Interface*
UPC *Usage Parameter Control*
URAD Unité de Raccordement d'Abonnés Déportés
URL *Uniform Ressource Locator*
UTP *Unshielded Twisted Pairs*
UU *CPCS User-to-User*
VBR *Variable Bit Rate*
VBR-rt *VBR Real Time*
VC *Virtual Connection*
VC *Virtual Contener*
VCC *Virtual Channel Connection*
VCI *Virtual Channel Identifier*
VIP *Visual Information Protocol*
VL Voie Logique
VLAN *Virtual Local Aera Network*
VoD *Video on Demand*
VPI *Virtual Path Identifier*
VPN *Virtual Private Network*
VR *Virtual Route*
VRC *Vertical Redundancy Check*
VT *Virtual Terminal*
VTAM *Virtual Telecommunication Access Mode*
VTOA *Voice and Telephony Over ATM*
WAN *Wide Area Network*
WAP *Wireless Application Protocol*
WDM *Wavelength Division Mode*
WWW *World Wide Web*
XID *eXchange IDentification command*

© Dunod – La photocopie non autorisée est un délit

Bibliographie

Afnor – Interconnexion de systèmes ouverts (OSI), recueil de normes françaises, Afnor (1991).

M. BOISSEAU, M. DEMANGE, J.-M. MUNIER – Réseaux ATM, Eyrolles (1995).

M. BOISSEAU, M. DEMANGE, J.-M. MUNIER – Réseaux haut débit - Eyrolles (1992).

D. COMER – Traduit de l'américain par J.A. HERNANDEZ, B. JOACHIM et R. JOLY– TCP/IP : Architecture, protocoles, applications, 4e édition, Dunod (2001).

J. HENSHALL, S. SHAW – OSI Les normes de communication entre systèmes ouverts, Editions Masson (1991).

D. KOFMAN, M. GAGNAIRE – Réseaux Haut Débit – InterEditions (1996).

C. MACCHI, J.-F. GUILBERT – Téléinformatique, Dunod informatique (1989).

D. MACKINNON, W. MCCRUM, D. SHEPPARD – Introduction à l'OSI, Afnor Technique (1991).

J.-L. MÉLIN – Pratique des réseaux - Eyrolles (1997).

H. NUSSBAUMER – Téléinformatique, volumes 1 à 4, Editions Presses Polytechniques Romandes (1991)

G. PUJOLLE – Les Réseaux, Eyrolles (2003).

G. PUJOLLE, D. SERET, D. DROMARD, E. HORLAIT – Réseaux et Télématique, Eyrolles (1989).

P. ROLIN, G. MARTINEAU, L. TOUTAIN, A. LEROY – Les réseaux, principes fondamentaux, Editions Hermes (1997).

P. ROLIN – Réseaux haut débit, Editions Hermes (1995).

A. TANENBAUM – Texte français par J.A. HERNANDEZ et R. JOLY – Réseaux, 3e édition, Dunod (1996).

K.-L. THAI, V. VÈQUE, S. ZNATY – Architecture des réseaux haut débit, Editions Hermes (1995).

L. TOUTAIN – Réseaux locaux et Internet, Editions Hermes (1996).

L'Echo des Recherches (périodique).

Réseaux & Télécoms (mensuel IDG Communication SA).

Revue des télécommunications (Alcatel).

Glossaire [1]

A

AAL (*ATM Adaptation Layer*) : Dans l'architecture ATM, la couche AAL est chargée de l'adaptation des unités de données des protocoles supérieurs en fonction des caractéristiques retenues pour le transfert (isochronisme...). Les services de la couche AAL se déclinent en AAL1 (Services à débit constant), AAL2 (Services sur connexion à débit variable), AAL3/4 (Services à débit variable pour le transfert de données) et AAL5 (Service sur connexion à débit variable). Voir *ATM*.

ABM (*Asynchronous Balanced Mode*) : Mode de communication supporté par HDLC (et par d'autres protocoles dérivés) concernant les communications point à point orientées poste à poste, dans lequel chaque station peut déclencher la transmission.

ABR (*Available Bit Rate*) : Classe de service dans ATM qui autorise une source à modifier son débit disponible en fonction d'information en provenance des commutateurs internes du réseau. Voir *CBR, UBR* et *VBR*.

Accès de base ou BRI *(Basic Rate Interface)* : Accès RNIS à 144 kbit/s, composé de deux canaux B à 64 kbit/s pour la transmission de la voix, de données et éventuellement d'images et d'un canal D à 16 kbit/s pour la transmission de la signalisation et de données (X.25). Voir aussi *RNIS et RNIS large bande.*

Accès Primaire ou PRI *(Primaire Rate Interface*) : Accès RNIS composé de 30 canaux B à 64 kbit/s (voix, données, images) et d'un canal D à 64 kbit/s (signalisation). Voir aussi *RNIS* et *RNIS large bande*.

Accusé de réception de bout en bout : Méthode d'acquittement et de reprise sur erreur dans laquelle ce sont les organes d'extrémité qui assurent le contrôle et la reprise sur erreur. Cette méthode d'acquittement simplifie la réalisation du sous-réseau physique de transport. En environnement faiblement perturbé, l'accusé de réception de bout en bout améliore les performances du réseau (diminution de la charge de traitement des nœuds intermédiaires). Voir *Accusé de réception local*.

Accusé de réception local : Méthode d'acquittement et de reprise sur erreur utilisée entre deux nœuds adjacents d'un réseau. Ce mode d'acquittement permet la reprise sur erreur au plus vite, elle minimise les délais de transmission de bout en bout en environnement perturbé. Voir *Accusé de réception de bout en bout*.

ACD (*Automatic Call Distributor*) : Système de distribution des appels téléphoniques entrants ou sortants.

1. Certains termes de ce glossaire sont extraits du dictionnaire CISCO des termes et acronymes réseaux, et reproduits ici avec l'aimable autorisation de la société CISCO System France.

Acheminement : Processus qui consiste à envoyer un bloc d'information (cellule, trame ou paquet) à sa destination finale via une ou plusieurs stations du réseau.

Ack (*Abréviation de acknowledgment*) : Message généralement envoyé par une unité du réseau à une autre pour accuser réception d'un événement (réception d'un message, par exemple). Voir *Accusé de réception local et de bout en bout, Nack*.

ACL (*Access Control List*) : Liste de contrôle des droits sur des fichiers, des accès réseau...

Adaptateur : Carte PC qui assure les communications du réseau à destination et en provenance d'une station. Synonyme NIC (*Network Interface Card*).

Adaptateur d'impédance : Voir *Balun.*

ADCCP (*Advanced Data Communication Control Protocol*) Protocole standard ANSI de liaison de données orienté bit.

ADCT (*Adaptative Discrete Cosinus Transform*) : Méthode de codage mise en œuvre dans le codage d'image et utilisant la transformation en cosinus discrète.

Administration de réseau : Terme générique utilisé pour décrire les systèmes ou les opérations qui permettent maintenir ou de dépanner un réseau.

ADPCM (*Adaptative Differential Pulse Coded Modulation*) : Méthode de compression de la voix. Chaque échantillon est codé par rapport à la valeur de l'échantillon précédent. Cette technique permet de réduire la bande à 16, 32 ou 48 kbit/s selon le nombre de bits utilisés pour coder la différence.

Adresse : Ensemble de données structurées utilisé pour identifier une entité unique, par exemple une station appartenant à un réseau.

Adresse de diffusion : Adresse permettant la transmission simultanée à toutes les stations d'un réseau (*broadcast*).

Adresse de groupe : Adresse de diffusion limitée permettant la transmission simultanée à plusieurs stations. Synonyme adresse multidestinataire (*multicast*).

Adresse Internet : Adresse sur 32 bits affectée aux interfaces réseaux utilisant le protocole IP (version 4). Cette adresse, écrite sous la forme de 4 octets séparés par des points en format décimal (*dotted decimal format*). Dans la version 6 d'IP la longueur d'adresse a été portée à 128 bits. Synonyme *Adresse IP*.

Adresse IP : voir *Adresse Internet*.

Adresse MAC : Également appelée *adresse physique*. Cette adresse sur 6 octets identifie de manière unique une machine sur un réseau, ces adresses sont en principe gérées par l'IEEE. L'adresse IEEE est divisée en deux champs. Le premier identifie le constructeur (attribué par l'IEEE) de l'interface matérielle, le second est un numéro séquentiel attribué par le constructeur dans une séquence déterminée par l'IEEE. L'adresse IEEE garantit l'unicité de l'adresse MAC attribuée.

Adresse multidestinataire : Adresse qui fait référence à plusieurs stations d'un réseau. Synonyme *Adresse de groupe*.

Adresse physique : Voir *Adresse MAC*.

Adresse source : Adresse d'une station de réseau jouant le rôle d'expéditeur. Cette adresse peut être une adresse physique (adresse MAC) ou une adresse d'accès à un réseau (adresse X.121) mais aussi la désignation d'un point d'accès à un service (SAP, *Service Access Point* dans la terminologie ISO).

Adresse unique : Adresse spécifiant une seule station d'un réseau (*Unicast*).

ADSL (*Asymetrical Data Subscriber Line*) : Technologie de traitement numérique du signal autorisant des débits élevés sur une simple ligne téléphonique. Les flux sont dissymétriques (640/6 000 kbit/s). À l'origine

prévu pour un service de vidéo à la demande, l'ADSL constitue aujourd'hui l'offre d'accès haut débit à Internet.

Affaiblissement du signal : Mesure le rapport entre la puissance du signal à l'entrée d'un système et celle en sortie. L'affaiblissement s'exprime en db (décibel).

AFI (*Authority and Format Identifier*) L'adresse réseau (*N-SAP, Network Service Access Point*) comporte 3 champs : l'AFI, l'IDI (*Initial Domain Identifier*), DSP *(Domain Specific Part*). Le champ AFI identifie l'autorité d'adressage, précise le format et la syntaxe de l'adresse. Par exemple : l'adresse X.121 est désignée par l'AFI = 38. Voir *IDI* et *DSP*.

Algorithme : Ensemble de règles opératoires et de procédés permettant de résoudre un problème par l'exécution d'un nombre fini d'opérations.

Algorithme de Dijkstra : Algorithme de routage par méthode de choix du plus court chemin pour déterminer l'arborescence de plus court chemin. Couramment utilisé dans les algorithmes de routage à état des liaisons. Voir aussi *Algorithmes de routage par vecteur de distance* et *Algorithmes de routage à état des liaisons*.

Algorithme de Karn : Algorithme qui améliore les estimations de temps de transmission aller-retour en permettant aux protocoles des couches Transport de différencier les mesures de bonne et de mauvaise qualité.

Algorithme de Nagle : Algorithme composé de deux formules de contrôle d'encombrement qui peuvent être utilisées dans les réseaux TCP. L'une réduit la fenêtre d'émission et l'autre limite l'envoi des petits datagrammes.

Algorithme de routage à état des liaisons : Algorithme selon lequel chaque routeur transmet des informations sur le coût de la connexion à chacun de ses voisins à tous les nœuds de l'interréseau. Ce type d'algorithme crée une vue cohérente du réseau et diminue les risques de boucles de routage. Voir aussi *Algorithme de routage par vecteur de distance, OSPF (Open Short Path First*), *IS-IS (Intermediate System to Intermediate System)*.

Algorithme de routage Bellman-Ford : Voir *Algorithme de routage par vecteur de distance*.

Algorithme de routage par vecteur de distance : Catégorie d'algorithmes de routage également appelé algorithme de routage Bellman-Ford qui itère sur le nombre de sauts d'une route pour trouver l'arbre recouvrant de plus court chemin. Ce type d'algorithme implique que chaque routeur envoie toute sa table de routage à chaque mise à jour, mais uniquement à ses voisins. Ces algoritmes peuvent générer des boucles de routage mais sont, au niveau calcul, plus simples que les algorithmes de routage d'état de liaison. Voir *Algorithme de routage d'état de liaison* et *Algorithme de Dijkstra.*

Algorithme du Lempel Ziv : Algorithme de compression de données.

Algorithme du spanning tree (ou arbre recouvrant) : Méthode d'acheminement utilisée dans les ponts entre réseaux locaux afin d'éviter la formation de boucles.

Alias : Nom de substitution utilisé pour identifier un objet en lieu et place de son nom complet.

ALOHA : Technique de transmission utilisée pour assurer le partage d'un support commun. La station qui a des données à transmettre les transmet sans se préoccuper de l'état du support. Si le message émis est brouillé par la présence d'un autre signal sur le support, il ne sera pas acquitté et sera retransmis ultérieurement. La technique ALOHA a été utilisée pour réaliser des communications entre différentes îles d'Hawaï.

Alternat : Voir *Half-duplex*.

© Dunod – La photocopie non autorisée est un délit

Amplitude : Valeur de crête d'un signal analogique ou numérique.

AMRC (Accès Multiple à Répartition de Code ou CDMA, *Code Division Multiple Access*) : une seule fréquence est utilisée et un code est attribué à chaque utilisateur. Cette technique est complexe mais accroît la capacité d'accueil des bases en simplifiant la gestion des fréquences.

AMRF (Accès Multiple à Répartition de Fréquence ou FDMA, *Frequency Division Multiple Access*) : Technique de multiplexage fréquentiel dans laquelle une fréquence est allouée à chaque utilisateur.

AMRT (Accès Multiple à Répartition dans le Temps ou TDMA, *Time Division Multiple Access*) : Technique de multiplexage temporel dans laquelle un intervalle de temps (IT) est alloué à chaque station. Plus souple que la précédente. Cette technique nécessite une parfaite synchronisation des stations.

Analyseur de réseau : Équipement matériel/logiciel qui offre diverses fonctionnalités (décodage de paquets spécifiques, tests de dépannage préprogrammés spécifiques, filtrages de paquets, transmissions de paquets, etc.).

Annuaire : Base de données mettant en correspondance une adresse réseau et un nom (résolution de nom).

Annulateur de modem : Voir *Éliminateur de modem*.

Anticipation : Voir *Fenêtre d'anticipation*.

Any LAN : Voir *IEEE 802.12*.

API (*Application Programming Interface*) : Interface de programmation qui met à disposition des programmeurs des primitives d'accès aux programmes systèmes.

Appel de procédure à distance (*RPC, Remote Procedure Call*) : Mode d'interaction par appel de procédures entre applications situées sur des machines différentes d'un réseau. Définit un cadre permettant de traduire les changements de contexte entre ces applications (sans que l'application appelante ait à gérer ce changement). Le RPC correspond à une mise en œuvre simple d'un modèle de type client/serveur.

Arbre recouvrant : Voir *Algorithme du spanning tree*.

Area : Voir *Région*.

ARP (*Address Resolution Protocol*) : Protocole Internet utilisé pour associer une adresse IP à une adresse MAC. Défini dans le document Internet RFC 826.

ARPANET : Premier réseau de communication par paquets, développé début des années soixante-dix. Le réseau ARPANET a évolué pour devenir Internet, et le terme ARPANET a été officiellement retiré en 1990

ARQ (*Automatic Repeat Request*) : Technique de communication dans laquelle le récepteur détecte les erreurs et demande la répétition de la transmission.

ART (Autorité de régulation des télécommunications) : créée par la loi du 27 juillet 1996, l'ART est chargée de définir le cadre de la concurrence entre les différents opérateurs.

Arythmique : Voir *Asynchrone*.

ASCII (*American Standard Code for International Interchange*) : Code utilisé pour la représentation des données. La longueur d'un mot du code est fixée à 7 bits (128 caractères, signes ou commandes représentables). Normalisé sous le nom de CCITT N° 5 ou (AI5, Alphabet International N° 5) le code ASCII a été étendu 8 bits pour représenter les caractères nationaux (ISO 8859-x) et dans les micro-ordinateurs des caractères semi-graphiques, on parle alors d'ASCII étendu ou encore d'ASCII IBM.

ASK (*Amplitude Shift Keying*) : Voir *Modulation d'amplitude*.

ASN.1 (*Abstract Syntax Notation One*) : Langage normalisé par l'ISO permettant de

décrire des types de données de façon totalement indépendante des structures et des techniques de représentation informatiques utilisées. (Norme internationale ISO 8824 de décembre 1987). Voir aussi *BER*.

Asynchrone : Se dit lorsque les événements gérés n'ont aucun lien temporel entre eux. Synonyme Arythmique. Voir *Transmission asynchrone, Terminal asynchrone.*

ATDM (*Asynchronous Time Division Multiplexing*) : Méthode de transmission d'information qui utilise le multiplexage par répartition temporelle, mais dans laquelle les tranches de temps sont, non pas pré-affectées à des émetteurs spécifiques, mais affectées le moment venu.

ATM (*Asynchronous Transfer Mode*) : Norme UIT de *relais de cellules* dans laquelle les informations destinées à différents types de services (voix, vidéo, données) sont transmises en paquets (cellules) de longueur fixe.

ATM Forum : Consortium de constructeurs, d'opérateurs, de consultants et d'utilisateurs chargés de définir et de promouvoir les technologies à base d'ATM.

Atténuation : Perte d'amplitude du signal sur les lignes et équipements de transmission. Synonyme *Affaiblissement*.

AUDIOTEX : Système de communication vocale (kiosque téléphonique) dans lequel l'opérateur téléphonique et le fournisseur de services se partagent les revenus.

AUI (*Attachment Unit Interface*) : Interface de raccordement de station. Câble IEEE 802.3 reliant le MAU (*Media Access Unit*) à la station. Le terme AUI peut également faire référence au connecteur de fond de panier de la station sur lequel un câble AUI peut être branché. Également appelé *câble émetteur-récepteur*.

Authentification : Méthode de sécurisation des échanges dans lequel l'identité des correspondants est vérifiée avant tout échange de données.

Authority zone : Voir *Zone d'autorité*.

Autocommutateur privé : Standard téléphonique installé dans les locaux de l'utilisateur. L'autocommutateur met en relation une ligne entrante ou sortante avec un poste téléphonique local ou deux postes téléphoniques locaux entre eux. Synonymes *PABX* et *PBX*

Avis : Terme qui désigne une norme édictée par le CCITT (UIT).

B

B-ISDN (*Broadband Integrated Service Digital Network*) : Voir *RNIS Large Bande.*

B-Router (*Bridge Router*) : Équipement assurant à la fois des fonctions de pont et de routeur entre deux réseaux. Synonymes *brouteur et pont-routeur*.

Backbone : Voir *Réseau dorsal*.

BAL (Abréviation de Boîte aux lettres) : Correspond à un espace de stockage dans lequel sont mémorisés les messages échangés entre deux processus ou deux correspondants (courrier électronique).

Balun (contraction de *balanced, unbalanced*) : Composant utilisé pour adapter deux lignes d'impédance caractéristique (Zc) différente, généralement une ligne à paires torsadées et un coaxial. Synonyme *Adaptateur d'impédance*.

Bande de base : Technologie de transmission native en réseau qui n'opère aucune translation du spectre. Ce terme est l'opposé du terme large bande où les données en transmettre sont translatées en fréquence (Modulation). Ethernet est un exemple de réseau à bande de base.

Bande de garde : Bande de fréquences utilisée entre deux canaux de communication qui permet de séparer les canaux pour empêcher toute interférence mutuelle. Voir *Intermodulation*.

Bande étroite : Voir *Bande de base*.

© Dunod – La photocopie non autorisée est un délit

Bande passante : Dans un système de transmission, les signaux sont transmis avec une distorsion faible dans une bande de fréquence comprise entre une fréquence basse (fréquence de coupure basse) et haute (fréquence de coupure haute). Au-delà de ces fréquences tous les signaux sont fortement atténués. On appelle bande passante d'un système l'espace de fréquence tel que tout signal appartenant à cet intervalle ne subisse qu'un affaiblissement déterminé par rapport à un signal de référence. L'affaiblissement s'exprime en décibel. La bande passante est généralement définie pour une atténuation de 3 dB (réduction de moitié de la puissance transmise).

Baud : Unité de mesure de rapidité de modulation, c'est-à-dire le nombre d'intervalles de temps élémentaires du signal numérique (nombre d'états).

Bc (*Commited Burst Size*) : Dans le relais de trames, le réseau ne traite pas la congestion, mais essaie de s'en protéger en limitant le débit des accès. Jusqu'à un certain volume de données (Bc*, Committed Burst Size*) le réseau assure le transfert de toutes les trames entrantes. Au-delà, le réseau autorise un certain débordement mais marque les trames en excès (bit DE, *Discard Eligibility*). Lorsque le volume transmis atteint une valeur prédéfinie à l'abonnement (Be*, Excess Burst*) toutes les trames en excédent sont éliminées en commençant par les trames marquées puis, si la congestion persiste et s'aggrave (congestion sévère), les trames non marquées et enfin les trames de signalisation.

BCD (*Binary Coded Decimal*) : Voir *Décimal Codé Binaire*.

BCS (*Bull Cabling System*) : Système de câblage préconisé par le constructeur BULL.

Be (*Excess Burst*) : Voir *Bc, (Committed Burst Size).*

BEB (*Binary Exponentiel Backoff*) : ou encore algorithme de ralentissement exponentiel, détermine, dans les réseaux IEEE 802.3, le délai aléatoire d'attente avant que la station ne retente, après collision, une émission.

BECN (*Backward Explicit Congestion Notification*) : Champ de la trame du relais de trames (1 bit) utilisé pour informer une source que son flux de données traverse au moins un commutateur en état de congestion. Voir *FECN* (*Forward Explicit Congestion Notification*).

BER (*Basic Encoding Rules*) : Règles de codage des unités de données décrites dans le langage ASN-1.

BER (*Bit Error Rate*) : Pourcentage de bits erronés reçus par rapport à la séquence de bits envoyés.

BGP (*Border Gateway Protocol*) : Protocole de routage interdomaine qui devrait remplacer le protocole EGP (*Exterior Gateway Protocol*).

Big-endian : Méthode de stockage ou de transmission de données dans laquelle le bit ou l'octet le plus significatif est présenté en premier (de gauche à droite). Voir aussi *Little-endian*.

Binaire : Système de codage de données composé uniquement de 0 et de 1.

Bit : Acronyme né de la contraction des mots anglais « *binary digit* ». Le bit est le plus petit élément d'information d'un système binaire transmissible, il peut prendre la valeur 0 ou 1. En principe le terme bit est invariable, mais l'usage le considère comme une unité classique et accorde le terme bit. Cependant on écrit 4 800 bits, mais 4,8 kbit ou encore 4 800 bit/s pour désigner le débit d'une ligne qui transmet 4 800 bits par seconde.

Bit par seconde (bit/s ou bps) : Unité de mesure du débit d'informations binaires. En principe l'utilisation de l'abréviation « bps » est à bannir à cause de la possible confusion avec byte par seconde.

Blindage : Tresse métallique de protection entourant un (câble coaxial) ou plusieurs conducteurs (paire coaxiale) afin de le protéger des rayonnements électromagnétiques. Le blindage est plus efficace au basse fréquence qu'un simple écrantage du câble. Voir *Ecran*.

BLU (Bande Latérale Unique) : Technique de modulation d'amplitude dans laquelle on a supprimé la porteuse et l'une des deux bandes latérales. Les signaux modulés en BLU sont moins sensibles à la dispersion du spectre.

Bluetooth : Technique de communication sans fil permettant à plusieurs systèmes de communiquer par liaison radio dans un rayon de quelques mètres.

Boucle de courant (*Current loop*) : Système de signalisation ou les interfaces connectées sont sensibles aux variations de courant et non aux variations de tension.

Boucle locale d'abonné : Ligne entre un abonné et le réseau de téléphone public.

Boucle Locale Radio (BLR) : Technique qui permet de raccorder un abonné du réseau téléphonique par une liaison hertzienne.

Bout en bout : Se dit d'une connexion ou d'un contrôle qui met directement en relation les entités communicantes. Par exemple, dans le cas d'un contrôle d'erreur de bout en bout en bout, la détection d'erreur et la reprise sont effectuées par le destinataire et non par les relais intermédiaires. La couche transport d'ISO et de TCP/IP sont des couches de bout en bout.

BPDU (*Bridge Protocol Data Unit*) : Paquet hello des protocoles « spanning-tree ». Voir aussi *PDU*.

BRI (*Basic Rate Interface*) : Voir *Accès de base*.

Bridge : Voir *Pont*.

Broadband : Voir *Large Bande*.

Broadcast : Voir *Adresse de diffusion*.

Brouteur : Voir *B-Router*.

Browser : Logiciel d'exploration permettant de naviguer sur Internet.

Bruit : Signal parasite sur un canal de communication. On distingue deux types de bruits : le bruit blanc (bruit naturel, occupant un large spectre, peu gênant) du bruit impulsionnel signal parasite intermittent provoquant une altération d'un bloc de données. Le rapport signal à bruit et la bande passante sont les deux éléments essentiels qui caractérisent un canal de transmission.

Bruit de quantification : La numérisation d'un signal analogique comprend les étapes d'échantillonnage, de quantification et de codage. La quantification est effectuée par rapport à une échelle (échelle de quantification) et la valeur de l'échantillon est exprimée par rapport à la valeur la plus proche de l'échelle. Cette méthode introduit une erreur de quantification dite bruit de quantification.

Burst : synonyme de rafale de trafic.

Bus à jeton : Architecture LAN utilisant un accès par passage de jeton sur une topologie en bus. Cette architecture est la base de la spécification LAN IEEE 802.4.

Byte : Voir *Octet*.

C

Câblage : Ensemble des éléments passifs permettant de raccorder les différents usagers d'un réseau local (câble, prises murales, panneaux de répartition ou de brassage...).

Câble : Support de transmission composé de fils ou de fibres optiques enveloppés sous une gaine de protection.

Câble blindé : Câble comportant une enveloppe métallique (tresse ou feuillard) dite blindage et assurant une protection contre les phénomènes électromagnétiques.

Câble coaxial : Câble blindé composé d'une gaine extérieure cylindrique en tresse métallique qui entoure un conducteur intérieur central (âme).

© Dunod – La photocopie non autorisée est un délit

Câble croisé : Voir *Éliminateur de modem*.

Câble optique : Voir *Fibre optique*.

Cache de noms : Méthode de stockage, par un nœud, de la correspondance entre un nom d'hôte distant et son adresse sur le réseau.

Call-back : Technique d'appel vers l'étranger consistant à appeler un opérateur étranger et à raccrocher. L'opérateur étranger établira alors la liaison avec le demandé et rappellera le demandeur. La communication est facturée au coût de l'opérateur étranger.

Canal B : En RNIS, canal duplex à 64 kbit/s utilisé pour transmettre la voix ou des données.

Canal D (*D_Channel*) : Canal de signalisation du RNIS fonctionnant en duplex et à 16 kbit/s (accès de base) ou 64 kbit/s (accès primaire).

Canal E : Canal RNIS de contrôle de l'accès au canal D (écho du canal D).

Canal H : Canal RNIS à débit primaire fonctionnant en *full duplex* à 384 kbit/s.

Canal sémaphore : Canal dédié à la signalisation entre deux ou plusieurs systèmes. Ex : le canal D du RNIS.

CAP (*Carrierless Amplitude/Phase modulation*) : Technique de codage.

Carrier signal : Voir *Porteuse*

Carrier : Voir *Opérateur de télécommunication*.

CAS (*Channel Associated Signaling*) : Signalisation de canaux numériques par vol de bits dans un IT de données (Trame T1) ou par IT réservé (Trame MIC, IT16).

CATV (*Cable Antenna TeleVision*) : Voir *Câble coaxial*.

CBDS (*Connectionless Broadband Data Service*) : Service d'interconnexion de réseaux WAN à haut débit fonctionnant en mode commutation de paquets non connectés. Synonyme *SMDS*.

CBR (*Constant Bit Rate*) : Dans un réseau ATM, débit négocié et garanti durant toute la durée de la connexion. Voir *ABR, UBR* et *VBR*.

CCBNT (*Circuit Commuté B Non Transparent*) : Service offert sur un réseau RNIS dans lequel une connexion numérique de bout en bout n'est pas garantie.

CCBT (*Circuit Commuté B Transparent*) : Service offert sur un réseau RNIS dans lequel une connexion numérique de bout en bout est garantie.

CCIR (*Comité Consultatif International des Radiocommunications*) : Organisme international de normalisation chargé d'émettre des avis sur la technique et la réglementation des radiocommunications, et notamment sur l'attribution des fréquences radio. Le CCIR a été intégré à l'UIT.

CCITT (*Comité Consultatif International Télégraphique et Téléphonique*) : Organisme international de normalisation en matière de télécommunications, qui développe des normes de communication sous forme, par exemple, d'avis en V (V.23, V.24...) pour les lignes analogiques ou en X (X.25...) pour les réseaux de données. Le CCITT est devenu l'UIT-T.

CCS (*Common Channel Signaling*) : Signalisation dans laquelle les informations de signalisation sont transmises sur un canal commun à toutes les communications. Le canal D du RNIS est un exemple de signalisation CCS.

Cellulaire : Voir *Radio Cellulaire*.

Cellule : Élément de base du multiplexage et de la communication ATM. Chaque cellule se compose d'un en-tête de 5 octets et de 48 octets de données utiles.

CGI (*Common Gateway Interface*) : Protocole de communication entre un serveur Web et une application.

CHAP (*Challenge Handshake Authentication Protocol*) : Fonction de sécurité qui

empêche tout accès non autorisé aux unités protégées. CHAP est un sous-protocole de PPP (*Point to Point Protocol*).

Chat (bavardage) : communication écrite en temps réel sur Internet entre deux ou plusieurs internautes.

Cheapernet : Terme faisant référence à la norme IEEE 802.3 10 Base2 ou au câble spécifié par cette norme. Thinnet, qui est également utilisé pour décrire cette norme, spécifie une version plus fine et moins onéreuse du câble Ethernet. Synonymes *câble noir, Ethernet capillaire, câble RG-58*.

Checksum : Voir *Somme de contrôle, CRC* et *FCS*.

Chiffrement : Technique de codage des informations qui applique un algorithme spécifique destiné à les rendre incompréhensibles à toute personne tentant de les lire illégalement. Le décryptage applique l'algorithme inverse et rend aux données leur format d'origine.

Chrominance : En télévision couleur, le terme chrominance désigne les informations de couleur R, V, B. Voir *Luminance.*

CIR (*Commited Information Rate*) : En Frame Relay, débit moyen d'information garanti

Circuit : Canal de communication entre plusieurs points.

Circuit Virtuel (CV) : Circuit logique établi pour assurer la fiabilité des communications entre deux stations d'un réseau.

Circuit Virtuel Commuté (CVC) : Circuit virtuel qui peut être établi dynamiquement à la demande. Inverse de *Circuit Virtuel Permanent* ou *PVC* (*Permanent Virtual Circuit*).

Circuit Virtuel Permanent (CVP ou PVC) : Circuit virtuel dont l'affectation est permanente.

Classe de service : Voir *COS*.

Client Serveur : Modèle d'organisation et de répartition des traitements entre un poste de travail « intelligent » et un serveur.

CLP (*Cell Loss Priority*) : Dans une cellule ATM, le bit CLP indique une cellule pouvant, en cas de congestion, être éliminée en priorité.

Cluster : Voir *Grappe*.

CMIP/CMIS (*Common Management information Protocol/Common Management Information Services*) : Interface de service/de protocole de gestion de réseaux de l'ISO créée et normalisée par l'ISO pour la gestion de réseaux hétérogènes.

CMOT (*CMIP Over TCP*) : Gestion d'un réseau TCP/IP par le protocole ISO CMIP.

CNLP/CLNS (*Connectionless Network Protocol/Connectionless Network Services*) : Protocole/Service de couche Réseau ISO qui ne demande pas l'établissement d'un circuit avant la transmission des données (ISO 8473). CLNP est l'équivalent ISO de IP.

CNLS (*ConnectionLess Network Service*) : Voir *Mode non connecté*.

Codage à la source : Technique dans laquelle à un élément d'information on fait correspondre une combinaison binaire. Voir *ASCII*.

Codage en ligne : Technique électrique qui consiste à modifier la forme du signal pour l'adapter aux exigences du support de transmission. Voir *Bande de base*.

Codage 4B5B : Technique de codage des informations binaires dans laquelle un groupe de 4 bits est remplacé par une combinaison binaire de 5 bits tel qu'il existe au moins deux transitions par groupe de 5 bits. Le codage 4B5B est utilisé dans les réseaux FDDI.

Codage biphase ou Manschester : Système de codage bipolaire développé à l'origine pour les réseaux Ethernet. Les informations de synchronisation sont incorporées dans le

© Dunod – La photocopie non autorisée est un délit

flot des données synchrones, à chaque temps bit correspond une transition du signal. La composante continue du codage biphase est nulle.

Codage différentiel : Technique de codage numérique selon laquelle une valeur binaire est signalée par un changement de signal, et non par un niveau de signal particulier.

Codage Manchester différentiel : Technique de codage numérique selon laquelle la transition du signal est de même sens que la précédente si le bit à coder est un 0 et de sens inverse si celui-ci est un 1. C'est la technique utilisée par les réseaux IEEE 802.5 et Token Ring.

Codage Manchester : Voir *Codage biphase*.

CODEC : Abréviation de Codeur-Décodeur. Équipement ou composant qui utilise généralement la modulation par impulsions codées pour transformer les signaux analogiques vocaux en signaux numériques, et vice versa.

Communauté : En protocole SNMP, groupe logique d'unités faisant partie du même domaine administratif.

Commutation de cellules : Forme particulière de la commutation de paquets. La cellule est « un paquet » de petite taille fixe. Voir *ATM*.

Commutation de circuits : Technique dans laquelle un circuit physique dédié, ou un intervalle de temps, entre l'émetteur et le récepteur est établi et maintenu durant tout l'échange.

Commutation de messages (*Messages switching*) : Technique de commutation consistant à diriger un message, dans son intégralité, de commutateur en commutateur, jusqu'à son destinataire.

Commutation de paquets (*Packets switching*) : Technique consistant à transmettre un message segmenté en blocs (paquets) entre commutateurs jusqu'à son destinataire. Chaque paquet pouvant être acheminé de manière indépendante (mode datagrammes) ou tous sur le même chemin (mode orienté connexion ou mode connecté). Voir aussi *Commutation de circuits et commutation de messages*.

Commutation Ethernet (*Switched Ethernet*) : Apparue dans le monde Ethernet la commutation a été mise en œuvre pour résoudre les problèmes d'effondrement des réseaux (collisions) et garantir à une communication une certaine bande passante, la technique de commutation est aujourd'hui mise en œuvre dans tous les types de réseaux. Dans cette technique, le hub est remplacé par un commutateur rapide qui met en relation directe ses différents ports d'accès selon une table dite table de commutation.

Commutation spatiale : Technique de commutation de circuits dans laquelle une relation une mise en relation de deux abonnés par juxtaposition de circuits liaisons physique est réalisée.

Commutation temporelle : Technique de mise en relation de deux abonnés par juxtaposition d'Intervalle de Temps (IT).

Compléments de service : Ensemble de services offerts par le réseau téléphonique RNIS qui correspondent essentiellement à un enrichissement de l'offre téléphonique traditionnelle. Ils fournissent une prestation optionnelle donnant lieu à facturation (abonnement ou appel par appel). Ces prestations sont, pour la plupart, déjà offertes sur les installations privées par l'intermédiaire des PABX.

Compression : Application à un ensemble de données d'un algorithme qui diminue l'espace/la largeur de bande nécessaire au stockage/à la transmission de cet ensemble.

Concentrateur : Équipement qui permet le regroupement de plusieurs canaux dans un réseau à topologie en étoile. Ce terme est également utilisé pour faire référence à une unité qui contient plusieurs modules d'équi-

pements de réseaux et d'interconnexion de réseaux.

Connecteur en T : Équipement en forme de T comportant deux connecteurs femelles et un connecteur mâle BNC.

CONS (*Connection-Oriented Network Service*) : Mode de transfert assurant aux protocoles des couches supérieures un fonctionnement orienté connexion. Voir *Mode orienté connexion*.

Contention : Synonyme *Collision* Situation dans laquelle les unités en réseau sont en concurrence pour l'accès au support physique. Voir aussi *Passage de jeton et commutation de circuits*.

Contrôle d'erreur : Technique permettant de garantir que les transmissions entre un émetteur et un destinataire sont exemptes d'erreur.

Contrôle de flux isarythmique : Technique de contrôle de flux basée sur la circulation d'une autorisation sur le réseau (permis).

Contrôle de flux par fenêtre : Méthode de contrôle de flux selon laquelle un récepteur donne à l'émetteur l'autorisation de transmettre des données jusqu'à ce qu'une fenêtre soit pleine. Lorsque la fenêtre est pleine, l'émetteur doit arrêter de transmettre jusqu'à ce que le récepteur ait déplacé la fenêtre. Cette méthode est utilisée notamment par TCP et d'autres protocoles de transport et par différents protocoles de couches de liaison.

Contrôle de flux : Technique permettant d'assurer qu'une entité émettrice à trop fort débit ne submerge une entité réceptrice (Asservissement de la cadence d'émission sur les capacités de réception du récepteur).

Contrôle de liaison logique (LLC, *Logical Link Control*) : Sous-couche définie par l'IEEE de la couche liaison de données de l'ISO qui gère le contrôle des erreurs, le contrôle du flux et les échanges de trames.

Contrôle de parité (ou d'imparité) : Technique de détection d'erreur qui consiste à ajouter au caractère transmis un bit à 1 ou à 0 (bit de parité) pour que la somme des bits à 1 transmis soit paire (contrôle de parité) ou impaire (contrôle d'imparité).

Cookie : Petit fichier téléchargé et contenant des informations sur le site web visité. Ces éléments seront réutilisés lors d'une prochaine connexion.

COS (*Class Of Service*) : Classe de service regroupement logique de caractéristiques de transmission affectées à un type de flux. Voir *ABR, CBR, UBR, VBR*.

Couche : Division fonctionnelle d'une architecture de communication. Une couche est un ensemble de services offert par une entité. Voir *OSI*.

Couche Application : Couche 7 du modèle de référence OSI. Cette couche met à disposition des programmes applicatifs des entités d'application (AE). Les principaux services de la couche application sont le courrier électronique (X.400), l'annuaire (X.500) et le transfert des fichiers (FTAM).

Couche Liaison de données : Couche 2 du modèle OSI. Ses principaux services sont la détection des erreurs et le contrôle du flux.

Couche physique : Couche 1 du modèle OSI qui définit les interfaces électriques, mécaniques et physiques du réseau, et les différents aspects du support du réseau.

Couche Présentation : Couche 6 du modèle OSI, qui définit la représentation des données entre deux entités de la couche Application.

Couche Réseau : Couche 3 du modèle OSI, qui concerne le routage des informations sur le réseau et les techniques d'adressage.

Couche Session : Couche 5 du modèle OSI, qui coordonne l'activité des sessions entre les applications, le contrôle des dialogues.

© Dunod – La photocopie non autorisée est un délit

Couche Transport : Couche 4 du modèle OSI, qui assure la fiabilité des transmissions entre les nœuds d'extrémité (EN). Cette couche assure également le contrôle d'erreur et le contrôle du flux des données, et utilise souvent des circuits virtuels pour garantir la fiabilité de la transmission des données.

Courant faible : Se dit des câblages qui ne mettent en œuvre que des signaux dont la tension maximale n'est que de quelques volts et dont l'objet est le transport d'information et non d'énergie (téléphone, données...). Voir *Courant fort*.

Courant fort : Se dit des installations dont l'objet essentiel est le transport d'énergie quels que soient les niveaux de tension transportés.

Courant porteur : Voir *Modulation.*

Courrier électronique : Voir *Messagerie électronique*.

Coût de routage : Valeur arbitraire utilisée pour déterminer le chemin de moindre coût (débit, nombre de sauts, taille des files d'attente...) possible entre un point d'origine et un point de destination. Voir aussi *Métrique de routage*.

CRC (*Cyclic Redundancy Check*) : Technique de recherche d'erreurs selon laquelle le destinataire d'une trame calcule un reste en divisant le contenu de la trame par un polynôme générateur principal, et compare le reste calculé (lui-même souvent appelé CRC) à la valeur calculée selon le même principe par l'émetteur et transmis avec l'unité de données. Si les deux valeurs sont différentes, le bloc reçu est rejeté et une retransmission est éventuellement redemandée. Synonyme *contrôle de redondance cyclique*. Voir *FCS*.

Critère de Nyquist : Relation entre la bande passante du système et nombre d'états significatifs. Voir *Rapidité de modulation, Baud*.

Crossbar : Ancien système de commutation électromagnétique utilisé dans les réseaux téléphoniques.

CSMA/CD (*Carrier Send Multiple Access Collision Detection*) : Réseau à accès multiple par détection de porteuse et détection de collisions. Procédure d'accès au canal par laquelle les stations voulant transmettre testent la présence d'un signal sur le canal. Si aucune activité électrique n'est détectée, les stations peuvent transmettre. Si deux stations transmettent simultanément, il se produit une *collision*, celle-ci est détectée par les stations concernées, qui arrêtent leur transmission et réalisent une retransmission après un temps d'attente aléatoire. L'accès CSMA/CD est utilisé par Ethernet et IEEE 802.3.

CT2 : Norme de radiotéléphone numérique sans fil. Définit des petits terminaux de poche permettant d'appeler par l'intermédiaire de bornes situées à une certaine distance, mais non de recevoir.

CTI (*Computer Telephony Integrated*) : Technique permettant l'interaction entre les éléments d'un appel téléphonique et une application informatique.

Current loop : Voir *Boucle de courant*.

CV : Voir *Circuit Virtuel*.

CVC : Voir *Circuit Virtuel Commuté*.

CVP : Voir *Circuit Virtuel Permanent*.

Cycles par seconde : Voir *Hertz.*

D

D_Channel : Voir *Canal D.*

Daemon : Programme qui s'exécute en arrière-plan.

Datagramme (*Datagram*) : Groupe logique d'information transmis sans qu'il ait été établi au préalable un circuit virtuel. La transmission n'est pas garantie, elle est dite *best effort*. Voir *Mode non connecté*.

DCB : Voir *Décimal Codé Binaire.*

DCE (*Data Circuit Equipment*) : Voir *ETCD*.

DCE (*Distributed Computing Environnement*) : Ensemble de spécifications de l'OSF (*Open System Fundation*) organisant le traitement d'applications réparties en environnement UNIX.

DCS 1800 (*Digital Cellular System 1 800 MHz*) : Norme de radiotéléphonie numérique dérivée du GSM.

DE (*Discard Eligibility*) : En cas de congestion, dans un réseau à relais de trames, les trames en excès sont purement et simplement éliminées par le réseau. Le bit *DE* est positionné par le réseau ou par les organes d'accès pour indiquer les trames à éliminer en priorité lors d'une congestion.

Débit binaire : Mesure la vitesse de transfert des informations sur un canal, ou caractéristiques de transfert d'un équipement. Le débit se mesure en bit/s.

Décibel (dB) : Unité logarithme exprimant le rapport entre deux grandeurs.

Décimal Codé Binaire (BCD*, Binary Coded Decimal* ou DCB*) :* Représentation binaire des nombres dans laquelle chaque chiffre est codé sur 4 bits. Le codage DCB est utilisé dans la représentation des adresses X.121.

DECT (*Digital European Cordless Telephon*) : Norme de radiotéléphonie numérique généralement utilisée pour la réalisation de téléphonie mobile d'entreprise. Le DCET utilise la bande des 1 800 MHz.

Dégroupage : Obligation qui est faite à l'opérateur historique (France Télécom) de mettre, moyennant redevance, à disposition des opérateurs alternatifs une partie du câblage de la boucle locale.

Délai de file d'attente : Temps pendant lequel les données doivent attendre d'être traitées par le système.

Délai de propagation : Délai nécessaire à la circulation des données sur le réseau entre leur source et leur destination finale.

Délimiteur : Voir *Fanion*.

Démodulation : Opération qui rend à un signal modulé sa forme d'origine. Les modems effectuent des fonctions de démodulation en prenant un signal analogique et en lui rendant sa forme numérique d'origine.

DES (*Data Encryption Standard*) : Technique de cryptographie développée par le *National Bureau of Standards* américain.

Détection d'erreur : Voir *Contrôle de parité, CRC, FCS*.

DHCP (*Dynamic Host Configuration Protocol*) : Service d'attribution dynamique d'une adresse IP à une station.

Dial-Up line : Se dit d'une connexion lorsque celle-ci est établie à la demande (connexion temporaire), généralement par l'intermédiaire du réseau téléphonique.

Diaphonie : Défaut de transmission provoqué par l'influence d'un canal de transmission sur un autre. Voir *Paradiaphonie*.

DIB (*Directory Information Base*) : Désigne l'annuaire distribué dans la norme X.500.

Diffusion (*Broadcast*) : Méthode de transmission de messages ou de fichiers à tous les destinataires d'un réseau.

DISC (*DISConnect*) : Trame non numérotée d'HDLC, l'un des ETTD prend l'initiative de la rupture de connexion.

Distorsion d'amplitude : Déformation du signal résultat du fait qu'un système ne transmet pas identiquement toutes les composantes du signal. Voir *Bande passante*.

Distorsion de phase : Problème découlant de la non-uniformité des vitesses de transmission des composants d'un signal sur un support de transmission (vitesse de groupe).

DIT (*Directory Information Tree*) : Organisation de la représentation arborescente des données dans la DIB d'X.500.

© Dunod – La photocopie non autorisée est un délit

DIX (*Digital Intel Xerox*) : Voir *Ethernet*

DLCI (*Data Link Connection Identifier*) : Étiquette identifiant une connexion dans les réseaux relais de trames (équivalent à la notion de NVL -Numéro de Voie Logique- dans X.25).

DNS (*Domain Name System*) : Nom du système d'annuaire distribué défini dans l'architecture TCP/IP et utilisé dans Internet.

DoD (*Department of Defense*) : Ministère de la défense des Etats Unis, à l'origine du protocole TCP/IP.

Domaine : Entité logique de gestion définie par l'administrateur du réseau qui regroupe un ensemble d'utilisateurs et de serveurs. En architecture Internet, partie d'une arborescence de noms.

Domotique : Ensemble de techniques informatiques en relation avec l'habitat privé.

Dorsal : Se dit d'un réseau fédérateur, synonyme de *backbone*.

DPAM (*Demand Priority Access Method*) : Technique d'accès utilisée dans les réseaux IEEE 802.12. Les stations sont raccordées à un concentrateur intelligent selon une topologie physique identique à celle du réseau 10 base T (réutilisation du câblage existant). Lorsqu'une station a des données à émettre, elle formule une requête au hub, qui lui alloue ou non le support.

DQDB (*Distributed Queue Dual Bus*) : Protocole de communication, développé par les Télécoms Australia, normalisé par le comité IEEE 802.6 pour les réseaux de type métropolitain. DQDB utilise la notion de cellule.

Drapeau : Voir *Fanion.*

Driver : Ensemble de programmes constituant un tout et destiné à assurer le fonctionnement d'un élément (carte réseau, imprimante...).

DSI (*Digital Speech Interpolation*) : Technique utilisée dans les réseaux voix/données pour récupérer, au profit de la donnée, les temps de silences de la voix.

DSP (*Domain Specific Part*) : Partie de l'adresse ISO qui contient un identificateur de zone (domaine). Voir *AFI, IDI*.

DSR (*Data Set Ready*) : Fil de la jonction RS-232-C activé lorsque le DCE (ou ETCD) est prêt à être utilisé.

DTE (*Data Terminal Equipment*) : Voir *ETTD*

DTMF (*Dual Tone Multifrequency*) : Système de numérotation téléphonique dans lequel chaque chiffre est représenté par deux fréquences, numérotation dite aussi Q.23.

Duplex : Mode de transmission permettant de transférer des informations dans les deux sens sur un même canal. Synonyme *bidirectionnel*.

Durée de vie (TTL, *Time To Live*) : Champ d'une unité de donnée qui contient un indicateur dit de durée de vie. Initialisé par l'émetteur, ce compteur est décrémenté par chaque nœud traversé. Quand la valeur atteint 0, le bloc de données est détruit. Cette technique évite qu'un bloc de données ne boucle dans un réseau.

E

E&M (*Earth & Mouth*) : Signalisation téléphonique RON/TRON (*Earth* pour RON, *Mouth* pour TRON). Voir *RON/TRON.*

E-mail : Courrier électronique

EBCDIC (*Extended Binary Coded Decimal Interchange Code*) : Code alphanumérique sur 8 bits développé par IBM.

Échantillonnage : Technique qui consiste à prélever, à intervalles réguliers, des échantillons d'un signal analogique afin de le convertir en signal numérique.

Écho : Signal parasite dû à la réflexion du signal lors d'une désadaptation d'impédance. L'écho engendre des ondes stationnaires, il génère des bits fantômes qui

peuvent, dans les réseaux locaux Ethernet provoquer des collisions.

Écran : Feuille métallique entourant une ou plusieurs paires torsadées afin de les protéger des rayonnements électromagnétiques. Voir *Blindage*.

EDI (*Electronic Data Interchange,* traduit en français par Échange de Données Informatisées) : Technique permettant de remplacer, pour les échanges entre entreprises ou organismes, les documents papier par des documents informatisés.

EFCN (*Explicit Forward Congestion Notification*) : Dans un réseau ATM, ce bit positionné par tout commutateur en état de congestion.

Égal à Égal (*Peer to Peer Ressource Sharing*) : Se dit d'un réseau local lorsque toutes les stations qui le composent peuvent partager des ressources et exécuter des applications locales.

Égalisation : Technique utilisée pour compenser les distorsions des canaux de communication. Synonyme *compensation*, *correction de distorsion*.

EGP (*Exterior Gateway Protocol*) : Protocole internet d'échange d'informations de routage entre systèmes autonomes. ce protocole est documenté dans le RFC 904.

EIR (*Excess Information Rate*) : Correspond au trafic maximum autorisé dans un réseau Frame Relay. Toutes les données émises dans l'intervalle CIR (*Constant Bit Rate*) et EIR sont marquées, positionnement du bit DE (*Discard Eligibity*) et éliminées en cas de congestion.

Éliminateur de modem : Dispositif de câblage permettant de simuler le dialogue à l'interface entre un modem et le terminal. L'éliminateur de modem permet de s'affranchir de l'utilisation d'un modem lors de transfert sur courte distance. Synonyme *Câble croisé*, *Null Modem*.

Émulateur de modem : Dispositif permettant de réaliser une liaison de terminaux ETTD sans modem. Synonyme *Null modem*.

Émulation de terminaux : Application réseau selon laquelle un ordinateur exploite un logiciel qui le présente à un hôte du réseau comme un terminal passif connecté directement.

En-tête : Données jointes à un bloc de données comportant les informations nécessaires au traitement, à l'acheminement ou au contrôle des données transmises. Ces informations de contrôle sont ajoutées avant les données lors de leur encapsulation pour transmission sur le réseau. Synonyme *PCI*. Voir ce terme.

Encapsulation : Technique qui consiste à transporter des unités de données d'un protocole dans une unité de données d'un autre protocole. Synonyme *Tunnel*.

Enregistreur : Élément d'un commutateur téléphonique qui reçoit et interprète la numérotation téléphonique.

Enveloppe : Voir *En-tête*.

Équilibrage de charges : Fonction qui permet à un routeur de répartir le trafic sur l'ensemble de ses interfaces qui sont à la même distance de l'adresse de destination. Les algorithmes d'équilibrage de charges les plus efficaces utilisent à la fois des informations de fiabilité et des informations de débit de ligne. L'équilibrage de charges augmente l'utilisation des segments du réseau, et donc sa bande passante effective.

ERBdB (Émetteur Récepteur en Bande de Base) : Équipement qui réalise une adaptation du signal au support (codage en ligne).

Erlang : Unité de mesure d'intensité de trafic d'un trafic. Un erlang correspond à l'occupation d'une ligne pendant une heure. La notion d'erlang est essentiellement utilisée en téléphonie où l'on admet qu'un poste téléphonique à un trafic, à l'heure de pointe, de 0,12 erlang.

© Dunod – La photocopie non autorisée est un délit

ERMES (*European Radio MEssaging System*) : Projet d'unification des systèmes de radiomessageries unilatérales européens (*pager*).

Erreur d'alignement : Dans les réseaux IEEE 802.3, erreur qui se produit lorsque le nombre total de bits d'un paquet reçu n'est un nombre entier d'octets. Ce type d'erreur est généralement provoqué par des problèmes de collision.

Erreur de quantification : Voir *Bruit de quantification*.

ETCD (Équipement de Terminaison de Circuit de Données) : Appareil adaptant les signaux émis par un équipement terminal aux caractéristiques de la ligne. Un modem peut être considéré comme un ETCD. Synonyme DCE (*Data Circuit Equipment*).

Ethernet : Réseau local à bande de base inventé par Xerox et développé conjointement par Xerox, Intel et Digital Equipment Corporation (Ethernet DIX). Les réseaux Ethernet fonctionnent à 10 Mbit/s et utilisent une méthode d'accès aux media de type CSMA/CD. Ethernet est normalisé par la norme IEEE 802-3.

Ethernet jaune : Voir *IEEE 802.3 10 base 5*.

ETR (*Early Token Release*) : Dans la version du réseau Token Ring à 4 Mbit/s, un seul jeton circule en permanence sur le support (système à trame unique). Dans les réseaux en anneau utilisant des débits supérieurs afin d'améliorer l'efficacité, lorsque la station maître a terminé d'émettre son message, elle régénère un jeton (système à trames multiples). De ce fait, plusieurs messages d'origines différentes et un jeton libre peuvent circuler en permanence sur le réseau. Le protocole ETR est utilisé dans les réseaux IEEE 802.5 à 16 Mbit/s et dans le réseau FDDI.

ETTD (Équipement Terminal de Traitement de Données) : Partie d'une station de données qui peut recevoir et/ou émettre des données, et qui assure la fonction de contrôle des communications de données selon certains protocoles. Le terme ETTD regroupe les ordinateurs, les traducteurs de protocole et les multiplexeurs. Synonyme DTE (*Data Terminal Equipment*).

Eutelsat (*European telecommunication satellite*) : Organisation européenne offrant des services internationaux (notamment téléphoniques) de communication par satellite.

Extranet : Réseau de communication interne à l'entreprise (Intranet) ouvert à certains éléments extérieurs à l'entreprise.

F

Fac Similé : Voir *Télécopieur*.

Facilities management (Externalisation) : Délégation plus ou moins totale des traitements informatiques et (ou) des télécommunications d'une entreprise à un prestataire de service.

Fading : En transmission radio, combinaison d'ondes directes et réfléchies qui module la réception et provoque un effet d'évanouissement.

Faisceau hertzien : Système de transmission radio à très haute fréquence se substituant aux systèmes filaires, les faisceaux hertziens permettent de réaliser des liaisons sans coût de génie civil.

Fanion : Information précédant et suivant une trame afin de la délimiter. Synonyme *Drapeau*, *Délimiteur*.

FCS (*Frame Check Sequence*) : Terme faisant référence aux caractères qui sont ajoutés à une trame pour la détection des erreurs. Synonyme *CRC*. Voir ce terme

FDDI (*Fiber Distributed Data Interface*) : Norme définie par l'ANSI et spécifiant un réseau à jeton à 100 Mbit/s utilisant un câble à fibre optique. Pour assurer la redondance de niveau physique, utilise une architecture à double anneau.

FDDI-II : Évolution de la norme FDDI proposée par l'ANSI. FDDI garantit une bande

passante minimale aux données des différentes stations (classe synchrone) mais ne garantit pas une récurrence temporelle entre les différentes émissions. De ce fait, FDDI-1 n'est pas susceptible d'assurer des transferts de données de type isochrone (voix, vidéo). FDDI-II superpose sur un même support, l'anneau FDDI, une voie asynchrone et synchrone (fonctionnement en mode paquets) et une voie isochrone (fonctionnement en mode circuits).

FDM (*Frequency Division Multiplexing*) : Voir *Multiplexage en fréquence*.

FECN (*Forward Explicit Congestion Notification*) : Les réseaux à relais de trames ne gèrent pas la congestion. Le contrôle de celle-ci est reporté aux organes d'extrémité. Lorsque le réseau est en état de congestion, il élimine purement et simplement les trames en excès et positionne un bit pour informer les organes d'extrémité de cet état. Les bits *FECN* (Notification de congestion en aval) et *BECN* (*Backward Explicit Congestion Notification*, notification de congestion en amont) sont utilisés pour signaler aux organes d'extrémité l'état de congestion du réseau.

Fédérateur : Voir *Réseau dorsal*.

Fenêtre d'anticipation : Technique de transmission dans laquelle les blocs de données sont émis sans attendre un accusé de réception. Le nombre de blocs pouvant être envoyés sans acquittement est désigné par fenêtre d'anticipation.

Fenêtre d'émission : Voir *Fenêtre d'anticipation*.

Fenêtre de réception : Nombre de blocs de données pouvant être reçus et éventuellement réordonnés par un système récepteur. Voir *Rejet sélectif, rejet simple*.

Fibre optique : Support de verre transportant les informations binaires en modulant un faisceau lumineux. La fibre optique autorise des débits élevés et permet de couvrir des distances importantes.

Fibre monomode : Fibre optique de diamètre relativement faible dans laquelle ne se propage qu'un seul faisceau de rayon lumineux. Ce type de fibre a une bande passante plus élevée que la fibre multimode, mais demande une source lumineuse ayant une plus faible largeur de spectre, par exemple LASER.

Fibre multimode : Fibre optique dans laquelle la propagation des informations s'effectue selon plusieurs chemins (modes).

FIFO (*First In, First Out*) : Mode de gestion des files d'attente selon lequel le premier message arrivé est le premier transmis.

File d'attente : Généralement, liste ordonnée d'éléments en attente de traitement. En routage, ensemble de paquets attendant d'être transmis sur une interface de routeur.

Firewall : Voir *Pare-feu.*

Flow control : Voir *Contrôle de flux.*

FM (*Frequency Modulation*) : Voir *Modulation de fréquence*.

Fondamental : Composante sinusoïdale de même fréquence que le signal périodique d'origine. Voir *Théorème de Fourier*.

Forwarding : Voir *Acheminement*.

Frame Interval (IFG, *Inter Frame Gap*) : Intervalle de temps minimal entre deux trames sur un réseau IEEE 802.3. Une station avant d'émettre doit détecter un silence d'au moins 9,6 μs (réseau à 10 Mbit/s). Ce temps minimal entre deux messages permet : d'une part, à l'électronique de bien discerner deux messages et, d'autre part, l'absorption d'éventuelles réflexions pour éviter la détection de collisions fantômes.

Frame Relay : Voir *Relais de trames*.

Frame Relay Forum : Consortium de constructeurs, d'opérateurs, de consultants et d'utilisateurs chargé de la définition et de la

© Dunod – La photocopie non autorisée est un délit

promotion des techniques et solutions basées sur le Frame Relay. Voir *Relais de Trames*.

Freeware : Logiciels gratuits

Fréquence : Nombre de cycles d'un signal transmis pendant une unité de temps donnée. La fréquence se mesure en Hertz (Hz) ou cycles par seconde.

Fréquence vocale : Désigne généralement la bande de fréquence nécessaire à la transmission de la voix analogique (300 à 3 400 Hz).

FSK (*Frequency Shift Keying*) : Voir *Modulation de fréquence*.

FTP (*File Transfer Protocol*) : Protocole de manipulation de fichiers l'environnement TCP/IP. FTP permet la création, la suppression et le transfert de fichiers.

FTP (*Folied Twister Pair*) : Câble à paires torsadées écranté.

Full duplex : Mode de fonctionnement d'une ligne ou d'un équipement dans lequel les informations sont transmises simultanément dans les deux sens. Synonyme *bidirectionnel simultané.*

G

Gateway : Voir *Passerelle*.

GFI (*General Format Identifier* ou IGF, *Identificateur Général de Format*) : Champ d'un paquet X.25 qui permet de définir certains paramètres de l'échange.

GIF (*Graphic Interchange Format*) : Mode de compression d'images numérisées en 256 couleurs.

Gigue (*Jitter*) : Variation du temps de transmission d'un signal.

GPRS (*General Packet Radio Services*) : Norme de transmission de données en mode paquets s'appuyant sur un réseau GSM.

GPS (*Global Positioning System*) : Système militaire de localisation par satellite (USA).

Grappe : Ensemble de terminaux passifs raccordés derrière un concentrateur.

GSM (*Global System for Mobile* communication, adaptation anglo-saxonne de Groupe Spécial Mobile) : Norme de radiocommunication numérique avec les mobiles. France Télécom (Orange) et SFR utilisent cette norme.

H

H.323 : Norme UIT pour le transfert de flux multimédia sur réseau sans garantie de service (mode datagrammes), utilisé dans la voix sur IP.

Hachage : Technique de cryptographie garantissant l'intégrité des données.

Half-duplex : Mode de communication dans lequel les données ne circulent que dans un sens à la fois. Synonymes *Alternat* et *Semi-duplex*.

Hand Over ou **handoff** : Fonction d'un système de radiocommunication qui permet à une station de se déplacer sans interruption de la communication.

Harmonique : Composante sinusoïdale d'un signal périodique non sinusoïdal. Voir *Théorème de Fourier.*

HDBn (Haute Densité Binaire d'ordre *n*) : Codage de type bipolaire dans lequel on introduit des bits fictifs (bit de viol et bit de bourrage) pour éviter une suite de plus de *n* bits consécutifs à zéro.

HDLC (*High Level Data Link Control*) : Protocole ISO standard de Liaison de données orienté bit, dérivé de SDLC. Spécifie une méthode d'encapsulation sur des liaisons de données séries synchrones.

Header : Voir *En-tête*.

HEC (*Header Error Control*) : Octet de contrôle d'erreur sur l'entête d'une cellule ATM. Le calcul du HEC utilise les techniques du CRC. L'HEC sert aussi au cadrage des cellules ATM.

Hertz : Mesure de fréquence ou de largeur de bande. Synonyme cy*cles par seconde.* Abréviation : *Hz.*

Hertzien : Voir *Faisceau hertzien*.

HIPPI (*High-Performance Parallel Interface*) : Interface à hautes performances définie par la norme ANSI X3T9.3/88-023.

HM (*Huffman Modified*) : Codage de Huffman utilisé dans les télécopieurs. Dans ce code, le codage des suites de points blancs ou noirs est préétabli. Voir *Huffman*.

Horloge : Élément d'un système de transmission qui détermine la cadence d'émission des symboles. Le rythme de l'horloge s'exprime en Hz.

HTML (*Hypertext Markup Language*) : Langage de description des pages de documents hypertextes mis à disposition sur les serveurs Web.

HTTP (*HyperText Transfer Protocol*) : Standard de protocole de transmission de données représentées en HTML (documents hypertextes)

Hub : Généralement équipement qui sert de centre à un réseau à topologie physique en étoile. En terminologie IEEE 802.3, un hub est un répéteur multiport Ethernet, qui est parfois appelé concentrateur. Le terme est également utilisé pour faire référence à une unité matérielle/logicielle contenant plusieurs modules (indépendants mais reliés les uns aux autres) de matériels de réseaux et d'interconnexion de réseaux.

Huffman (codage) : Méthode de compression basée sur les occurrences d'apparition d'un symbole, d'une combinaison binaire ou autre. Le symbole le plus fréquemment employé sera codé avec un nombre minimum de bits. Le code de Huffman est utilisé dans la télécopie.

I

ICMP (*Internet Control Message Protocol*) : Protocole internet qui fournit des messages d'erreur et d'autres informations concernant le traitement des paquets IP. Documenté dans le RFC 792.

IDI (*Initial Domain Identifier*) : Élément de l'adresse réseau de l'ISO, IDI identifie le domaine dans lequel s'applique l'adresse. C'est par exemple le code pays de X.121. Voir AFI, DSP.

IDP (*Initial Domain Part*) : Partie d'une adresse SNPA (*SubNetwork Point of Attachement*) qui définit l'autorité de gestion de l'espace d'adressage.

IEEE (*Institute of Electrical and Electronic Engineers*) : Organisation professionnelle américaine qui définit, entre autres, des normes réseau. Ses normes LAN sont actuellement les plus suivies et comprennent notamment des protocoles similaires ou pratiquement équivalant aux protocoles Ethernet et Token Ring.

IEEE 802.2 : Protocole IEEE qui spécifie une implémentation de la sous-couche Contrôle de liaison logique de la couche Liaison de données (couche LLC). Ce protocole gère les erreurs, le format des données, le contrôle de flux et l'interface de service de Couche 3, il est utilisé dans les normes de réseaux locaux (LAN) comme IEEE 802.3 et IEEE 802.5.

IEEE 802.3 Protocole IEEE qui spécifie une implémentation de la couche Physique et de la sous-couche MAC de la couche liaison de données, Ce protocole utilise l'accès CSMA/CD à différentes vitesses sur différents supports physiques. L'une de ses variantes physiques (10 base5) est très semblable à Ethernet.

IEEE 802.3 10 Base5 : Norme IEEE 802.3 Ethernet. Transmission en bande de base utilisant comme support un câble coaxial épais. Débit de 10 Mbit/s et longueur maximale d'un segment limitée à 500 mètres.

IEEE 802.3 10 Base2 : Norme IEEE 802.3 Ethernet utilisant pour support un câble coaxial fin. Longueur maximale d'un segment limitée à 185 mètres. Débit de 10 Mbit/s.

© Dunod – La photocopie non autorisée est un délit

IEEE 802.3 1Base5 : Première version du réseau Ethernet sur paires torsadées. Le débit était limité à 1 Mbit/s. Synonyme *StarLAN*.

IEEE 802.3 10 BaseT : Norme IEEE 802.3 qui utilise un câblage à paires torsadées non blindées et à un débit de 10 Mbit/s. Évolution du réseau StarLAN.

IEEE 802.4 : Protocole IEEE qui spécifie une implémentation de la couche Physique et de la sous-couche MAC de la couche Liaison de données. Ce protocole utilise la technique de passage de jeton sur une topologie en bus.

IEEE 802.5 : Protocole IEEE qui spécifie une implémentation de la couche Physique et de la sous-couche MAC de la couche Liaison de données. Ce protocole utilise la technique de passage de jeton à 4 ou 16 Mbit/s sur un câblage à paires torsadées blindées et est très semblable au Token Ring IBM.

IEEE 802.6 : Spécification MAN (réseau métropolitain) IEEE basée sur la technologie DQDB. Ce protocole supporte des vitesses de transmission comprises entre 1,5 et 155 Mbit/s.

IEEE 802.12 (*100 VG Any Lan*) : VG Lan est un réseau local à 100 Mbit/s compatible, au niveau des formats de trames, avec Ethernet ou Token Ring (selon configuration), il implémente un nouveau protocole d'accès fondé sur la méthode du polling. Le terme *Any Lan* provient de sa double compatibilité, se contentant de simples paires torsadées de qualité vocale (*VG*, *Voice Grade*), le 100 VG Any Lan offre un débit de 100 Mbit/s et un accès déterministe. Il semble bien tolérer le trafic de type isochrone.

IFG (*Inter Frame Gap*) : Temps de silence entre deux trames Ethernet. Voir *Frame Interval*.

IGP (*Interior Gateway Protocol*) : Protocole Internet utilisé pour échanger des informations de routage au sein d'un système autonome. Exemple : IGRP, RIP et OSPF.

IGRP (*Interior Gateway Routing Protocol*) : Protocole IGP développé par Cisco Systems pour résoudre les problèmes associés au routage dans de gros réseaux hétérogènes.

Impédance : Caractéristique électrique d'un système dépendant directement de sa résistance, de sa capacitance, de son inductance et de la fréquence. L'impédance s'exprime en ohm (Ω).

Impédance caractéristique (Zc) : L'impédance caractéristique est l'impédance d'une ligne de longueur infinie. On montre que lorsqu'une ligne de longueur finie est refermée sur un récepteur, dont l'impédance Zr est égale à l'impédance caractéristique de la ligne, celle-ci se comporte comme une ligne de longueur infinie, on dit alors que la ligne est adaptée. Voir *Adaptation d'impédance*.

Infrarouge : Bande d'ondes électromagnétiques dont la plage de fréquences se situe au-dessus de celle des micro-ondes, mais en dessous du spectre visible, et utilisée pour la transmission d'informations sans fil sur de très courtes distances.

Interface : Connexion entre deux équipements ou systèmes. En télécommunications, connexion à un réseau. Également, frontière entre des couches adjacentes du modèle OSI. En téléphonie, frontière définie par une communauté des caractéristiques de signaux, de caractéristiques d'interconnexion physique, et de contenu des signaux échangés.

Interférences : Parasites perturbant les signaux circulant sur des canaux de communication.

Intermodulation : Interférence entre deux signaux l'un modulant l'autre et vice versa. Pour éviter l'intermodulation, les spectres de fréquences des deux signaux doivent être suffisamment espacés (*Bande de garde*).

International Standards Organization : Voir *ISO*.

Internetworking : Interconnexion de réseaux.

Interopérabilité : Possibilité, pour des équipements de différents constructeurs, de communiquer entre eux.

Intranet : Réseau d'entreprise mettant en œuvre les mêmes technologies que le réseau Internet.

Invitation à émettre (*polling*) : Dans une relation maître/esclave, l'invitation à émettre est envoyée par la station maître à la station esclave pour l'inviter à envoyer ses informations. Cette solution évite les problèmes de conflits entre machines.

Invitation à recevoir (*selecting*) : Dans une relation maître/esclave, l'invitation à recevoir est envoyée par la station maître à la station esclave pour lui indiquer qu'elle a un message à lui envoyer.

IP (*Internet Protocol*) : Protocole de couche 3 (couche Réseau) contenant des informations d'adressage et certaines informations de contrôle permettant le routage des paquets. Documenté dans le RFC 791. Synonyme *protocole interréseau*.

IPNS (*ISDN PABX Networking Specification*) : Système de signalisation entre PABX hétérogènes développé par Alcatel et Siemens et à l'origine de la norme Q-SIG.

IRC (*Internet Relay Chat*) : Voir *Chat*.

Iridium : Système de téléphonie par satellites comprenant 66 satellites développé par Motorola. Fermé 3 mois après sa mise en service pour faute de client, Iriduim a été racheté par Boeing, le principal client est l'US-Army.

ISDN (*Integrated Services Digital Network*) : Voir *RNIS*.

ISO (*Interconnexion de systèmes ouverts*) : Traduction française de OSI, ne devrait jamais être utilisée, car il y alors confusion entre le modèle (OSI en anglais et ISO en français) et l'organisme (ISO en anglais et OSI en français). Voir *OSI*.

ISO (*International Standard Organization*) : Organisme international chargé de la mise au point d'une vaste gamme de normes, dont celles concernant les réseaux. L'ISO a mis au point le modèle de référence le plus connu, appelé *modèle OSI*.

Isochrone : Signaux ou réseaux utilisant une référence temporelle unique.

IT (*Intervalle de Temps*) : Dans le multiplexage temporel, l'IT correspond au temps attribué à chaque source pour émettre ses données.

J

Jabber : Condition d'erreur qui survient lorsqu'une unité du réseau transmet continuellement des informations parasites. En protocole IEEE 802.3, paquet de données dont la longueur dépasse celle autorisée par la norme (1 518 octets).

Jarretière : Câble souple utilisé dans les panneaux de brassage (répartiteurs) pour relier un abonné à un service (téléphonique, commutateur ou hub Ethernet...)

Jeton : Trame d'informations de contrôle dont la possession donne à une station du réseau le droit d'émettre.

Jeton adressé : Technique du jeton utilisé dans les réseaux IEEE 802.4. Dans ces réseaux le jeton contient l'adresse de la station à laquelle le droit de parole est attribué. Le jeton circule de la station de plus faible adresse à celle de plus forte adresse, formant ainsi un anneau virtuel sur le bus (anneau logique/bus physique).

Jeton non adressé : Technique de distribution du droit à parole utilisée dans les réseaux IEEE 802.5. Dans un tel système, les informations (trames) transitent par toutes les stations actives. Le droit à parole est matérialisé par une trame particulière « *le jeton ou token* ». Celui-ci circule en permanence de station en station. Une station qui reçoit le jeton peut émettre une ou plusieurs trames (station maître). Si elle n'a rien

© Dunod – La photocopie non autorisée est un délit

à émettre, elle se contente de répéter le jeton (station répéteur).

Jitter : Voir *Gigue*.

Joncteur : Élement de raccordement d'une ligne ou d'un circuit à un organe de traitement.

JPEG (*Joint Photographic Experts Group*) : Norme de compression très performante d'images fixes numérisées en 16,7 millions de couleurs (12 bits par pixel).

K

Kerberos : Protocole d'authentification d'un utilisateur développé par le MIT (Massachussetts Institute of Technology).

Kermit : Protocole de transfert de fichiers en mode asynchrone et d'émulation de terminaux. Développé par l'université de Colombia, Kermit est du domaine public.

L

LAN (*Local Area Network*) : Voir *Réseau local*.

LAN émulation : Technique qui permet la réalisation d'un réseau local virtuel sur une infrastructure à base d'ATM. Cette technique masque aux couches supérieures l'emploi d'un réseau ATM en lieu et place d'un LAN traditionnel (*legacy LAN*).

LAP-B (*Link Access Protocol, Balanced*) : Procédure dérivée de HDLC, version CCITT X.25 d'un protocole de liaison de données orienté bit.

LAP-D (*Link Access Protocol D*) : Protocole de couche Liaison de données RNIS pour canal D. Ce protocole est dérivé du protocole LAP-B CCITT X.25 et conçu essentiellement pour résoudre les problèmes de signalisation de l'accès de base RNIS. Défini par les avis CCITT Q.920 et Q.921.

Large bande : Par opposition aux transmissions en bande de base, technologie de transmission qui effectue une translation du spectre du signal (Modulation).

Largeur de bande : Espace de fréquence occupé par un signal (fondamental et harmoniques). Synonyme *Spectre de fréquence*.

Larsen : Du nom de son découvreur, l'effet Larsen correspond au couplage entre un microphone et un système amplificateur qui provoque une boucle de réaction positive et fait entrer le système en oscillation. l'effet Larsen se manifeste par un sifflement aigu.

LASER (*Light Amplification by Stimulated Emission of Radiation*) : Équipement de transmission dans lequel un matériau actif est excité par un stimulant externe pour produire un faisceau étroit de lumière cohérente qui peut être modulé en impulsions pour transporter des données.

LCR (*Least Cost Routing*) : Logiciel embarqué dans les PABX et destiné à choisir l'opérateur de moindre coût pour établir une communication téléphonique.

LDAP (*Lightweight Directory Access Protocol*) : Protocole fédérateur d'accès aux services d'annuaires.

LED (*Light Emitting Diode*) : Composant électronique qui sous l'effet d'un courant émet une radiation lumineuse.

Lempel Ziv : Voir *Algorithme du Lempel Ziv.*

LIA (*Liaison Inter-Automatique*) : Liaison établie entre deux autocommutateurs téléphoniques pour acheminer des communications téléphoniques.

Liaison : Canal de communication de réseaux composé d'un circuit ou d'une voie de transmission, et comprenant tous les équipements entre l'émetteur et le récepteur. Terme souvent utilisé pour faire référence à une connexion WAN. Parfois appelée *ligne*.

Liaison analogique et liaison numérique : Désigne un type de liaison. Une liaison est dite analogique lorsque l'interface usager est du type analogique (modem), elle est dite numérique quand l'interface usager est numérique (CODEC ou ERBdB).

Liaison d'abonné : Liaison dédiée qui relie un abonné d'un réseau à un point d'accès de ce réseau.

Liaison de données (*data link*) : Liaison affectée à une transmission numérique. Cette expression désigne surtout la couche 2 du modèle OSI de l'ISO.

Ligne commutée : Circuit de communication établi par une connexion via un réseau à commutation de circuits utilisant l'infrastructure du réseau téléphonique.

Ligne multipoint : Ligne de communication reliant physiquement plusieurs équipements.

Link status (état de la ligne) : Signal particulier utilisé dans les réseaux 802.3 10 base T pour contrôler la continuité du lien entre le hub et la station.

Liste d'accès : Liste tenue à jour par les routeurs afin de contrôler l'accès à un certain nombre de services (par exemple pour empêcher les paquets ayant une certaine adresse IP de sortir sur une interface particulière du routeur).

Little-endian : Méthode de stockage ou de transmission des données dans laquelle le bit ou l'octet le moins significatif est présenté en premier. Voir aussi *Big-endian*.

LLC (*Logical Link Control*) : Voir *Contrôle de liaison logique*.

Logical link control : Voir *Sous-couche LLC*.

Loi-A : Norme CCITT (UIT-T) de compression-extension utilisée lors de la conversion de signaux analogiques/numériques sur les systèmes à modulation par impulsion et codage. Cette norme est surtout utilisée dans les réseaux téléphoniques européens. La loi-A est incompatible avec la loi-mu en vigueur en Amérique du Nord et au Japon.

Loi-mu : Norme nord-américaine de compression-extension utilisée lors de la conversion de signaux analogiques/numériques sur les systèmes à modulation par impulsion et codage.

Longueur d'IT : Exprime en bits le nombre de bits transporté durant un intervalle de temps dans un système de multiplexage temporel.

Longueur de mot : La longueur de mot exprime le nombre de bits qui code un symbole. Par exemple le code ASCII utilise des mots dont la longueur est de 7 bits.

Luminance : En télévision couleur, le signal de luminance représente l'image monochrome ou échelle des gris. Voir *Chrominance*.

M

MAC (*Medium Access Control*) : Dans les réseaux locaux, sous-couche de niveau liaison gérant l'accès au support. Voir *Contrôle d'accès au support.*

Mail Box : Voir *Boîtes à lettres (BAL)*.

Maillage : Définit la connectivité d'un nœud du réseau, le nœud pouvant être atteint par différents liens.

Mainframe : Voir *Ordinateur Central*.

MAN (*Metropolitan Area Network*) : Réseau de transmission couvrant généralement une ville et ses environs. Autorise l'interconnexion de plusieurs réseaux locaux.

Manchester : Voir *Codage Biphase*.

MAQ (*Modulation en Amplitude et à porteuse en Quadrature*) : Technique de modulation qui combine la modulation d'amplitude et de phase.

Masque de sous-réseau : Champ de bits qui permet d'étendre l'adresse réseau d'IP. Ce champ est utilisé pour spécifier des sous-réseaux du réseau principal.

MAU : **1)** *Medium Attachment Unit* : Équipement de raccordement dans un réseau Ethernet. Synonyme *Transceiver*. **2)** *Multiple Access Unit* : Hub dans les réseaux 802.5 (Token Ring).

© Dunod – La photocopie non autorisée est un délit

Media : Supports physiques véhiculant les signaux de transmission : paires torsadées, câbles à fibres optiques, câbles coaxiaux et atmosphère (qui sert de support de transmission aux micro-ondes, aux rayons laser et aux transmissions infrarouges).

Mémoire-tampon (*buffer*) : Zone de mémoire utilisée pour la gestion des données en transit. Les mémoires-tampon sont souvent utilisées pour compenser les différences de vitesse de traitement entre les stations du réseau. Les données transmises par rafales peuvent être stockées dans une mémoire-tampon jusqu'à ce qu'elles puissent être prises en compte par les périphériques moins rapides.

Messagerie électronique : Technique permettant aux utilisateurs d'échanger des messages sur un certain nombre de types de réseau en utilisant des protocoles variés. Synonyme *Courrier électronique*.

Méthode d'accès : Algorithme de partage du support physique dans un réseau local. Voir *MAC*.

Métrique de routage : Valeur qui permet à un algorithme de routage de déterminer qu'une route est meilleure qu'une autre. Ces informations sont stockées dans des tables de routage. Les métriques peuvent être exprimées en fonction du taux d'erreur de la liaison, du délai de transmission, de la bande passante, la charge, du MTU, du nombre de sauts.

Metropolitan Area Network : Voir *MAN*

MF (*Modulation de Fréquence*) : Voir *Modulation de fréquence*.

MHS (*Message Handling System*, ISO 10021, CCITT) : implémente un service de messagerie en mode non connecté ; en cas d'absence du destinataire, le message est délivré dans sa boîte à lettres.

MIB (*Management Information Base*) : Base de données d'information d'administration des réseaux.

MIC (*Modulation par Impulsions et Codage*) : Technique de transmission des informations analogiques sous forme numérique par échantillonnage et codage des échantillons d'aide d'un nombre fixe de bits. Synonyme *PCM Pulse Code Modulation*. Voir aussi *Connecteur d'interface au support.*

MICDA (*MIC Différentielle Adaptable*) : Processus tirant profit de la forte corrélation statistique entre des échantillons de voix consécutifs afin de créer une échelle de quantification variable. La MICDA encode des échantillons de voix analogiques en signaux numériques de haute qualité.

Micro-ondes : Ondes électromagnétiques de fréquences comprises entre 1 et 30 gigahertz. Les réseaux exploitant ce type d'ondes reposent sur une technologie récente, mais de plus en plus employée en raison de son faible coût et de sa bande passante importante.

Microprogramme : Instructions logicielles enregistrées de manière permanente ou semi-permanente en mémoire morte (ROM). Synonyme *firmware*.

Middleware : Ensemble de logiciels situé entre le système d'exploitation et les programmes d'application.

MIME (*Multipurpose Internet Mail Extension*) : Logiciel de diffusion de messages électroniques au format binaire. Permet l'encapsulation de différents formats de données dans un même message.

Minitel : Terminal asynchrone défini pour l'accès au vidéotext.

MNP (*Microcom Network Protocol*) : Série de protocoles intégrés aux modems proposée par la société Microcom ayant pour objectif d'améliorer la transmission sur une liaison de données. Les plus connus sont MNP4, détection d'erreur, et MNP5, compression de données qui ont été repris par les instances de normalisation.

Mode non connecté (CNLS, *Connection-Less Network Service*) : Mode dans lequel les transferts de données sont effectués à la demande. Chaque bloc de données est transféré indépendamment, il n'y a aucune garantie de délivrance (mode pour le mieux ou *best effort*). Ce mode est généralement appelé mode datagramme.

Mode orienté connexion (CONS, *Connection-Oriented Network Service*) : Mode dans lequel les transferts de données demandent l'établissement préalable d'un circuit virtuel (CV). Le mode orienté connexion est généralement désigné plus simplement par mode connecté.

Modèle OSI (*Open System Interconnection*) : Modèle architectural de réseaux développé par l'ISO et le CCITT. Le modèle se compose de sept couches, dont chacune spécifie des fonctions réseau particulières comme l'adressage, le contrôle du flux, la gestion des erreurs, l'encapsulation et la fiabilité du transfert des messages. La couche la plus haute (la couche Application) est la plus proche de l'utilisateur, et la couche la plus basse (la couche Physique) la plus proche de la technologie des supports. Le modèle OSI est universellement utilisé pour apprendre et comprendre les fonctionnalités des réseaux.

MODEM (MOdulateur-DEModulateur) : Boîtier qui convertit les signaux numériques en vue de leur transmission sur des installations de communication analogique, et vice versa.

Modulation : Technique par laquelle un signal à transmettre modifie un paramètre d'un autre signal, appelé porteuse. Voir *Modulation d'amplitude, modulation de fréquence, modulation de phase.*

Modulation d'amplitude (ASK, *Amplitude Shift Keying*) : Technique de modulation dans laquelle le signal à transmettre n'est pas transmis directement. Ce signal est utilisé pour modifier l'amplitude d'un autre, appelé porteuse.

Modulation de fréquence (FSK, *Frequency Shift Keying*) : Technique de modulation dans laquelle le signal modulant modifie la fréquence du signal porteur. Du fait de la grande largeur de bande du signal modulé, la modulation de fréquence n'est utilisée que dans les modems à faible débit.

Modulation de phase (PSK, *Phase Shift Keying*) : Technique de modulation dans laquelle le signal modulant modifie la phase du signal porteur. Généralement, les modems utilisent une combinaison de la modulation d'amplitude et de phase appelée MAQ (Modulation en Amplitude et Quadrature).

Modulation par impulsions codées : Voir *MIC*.

MP3 : Morme de compression du son.

MPEG (*Move Picture Experts Group*) : Format de compression vidéo utilisé dans la télévision numérique.

MRT (*Multiplexage à Répartition Temporelle*) : Voir *Multiplexage temporel*.

MRT Asynchrone (*Multiplexage à répartition temporelle asynchrone*) : Voir *ATDM*.

MTA (*Message Transfer Agent*) : En messagerie entité (logiciel) qui assure la circulation des messages entre agents utilisateurs.

MTBF (*Mean Time Between Failure*) : Temps moyen de bon fonctionnement d'un équipement.

MTS (*Message Transfer System*) : En messagerie ensemble des MTA appartenant à un même domaine.

MTTR (*Mean Time To Repair*) : Temps moyens de remise en état d'un équipement.

MTU (*Maximum Transfer Unit*) : Taille maximum des paquets, exprimée en octets, qu'un réseau peut transmettre.

Multicast : Voir *Adresse de groupe.*

Multimedia : Flux d'information qui associe le texte, le son, l'image et la vidéo.

© Dunod – La photocopie non autorisée est un délit

Multiplexage : Technique permettant de faire passer plusieurs communications sur un même canal de transmission.

Multiplexage à répartition temporelle asynchrone : Voir *ATDM*.

Multiplexage de position : Technique dans laquelle les différents blocs de données sont identifiés par leur position dans une trame. Le multiplexage temporel est une technique de multiplexage de position.

Multiplexage en fréquence : Technique qui consiste à découper la bande passante d'un canal en plusieurs sous-bandes, chacune étant affectée à une voie. Le multiplexage en fréquence correspond à une juxtaposition fréquentielle de voies et à une superposition des signaux dans le temps.

Multiplexage par étiquette : Technique dans laquelle les blocs de données ne sont pas identifiés par leur position dans une trame mais par un identificateur appelé étiquette. Cette étiquette peut, par exemple, être le numéro de voie logique utilisé dans X.25 pour identifier les paquets sur une liaison.

Multiplexage spatial : Voir *Multiplexage en fréquence*.

Multiplexage temporel : Technique permettant d'affecter à des informations provenant de différents canaux une largeur de bande sur un support unique, selon un système d'affectation de tranches de temps (IT, Intervalle de Temps). Le multiplexage temporel correspond à une juxtaposition des voies dans le temps et à l'utilisation d'un même espace fréquentiel.

Multiplexeur statistique (*STDM, Statistical Time Division Multiplexing*) : Équipement de multiplexage qui affecte de manière dynamique la capacité d'une ligne uniquement aux canaux d'entrée actifs, et permet de connecter davantage de stations qu'un multiplexeur traditionnel. Également appelé *multiplexeur statistique temporel*.

N

NAck (*Negative Acknoledge*) : Acquittement négatif. Voir *Ack*.

Named pipes (*pipe nommé*) : Canal virtuel de communication permettant une communication directe entre deux applications.

Navigateur : Voir *Browser*.

NDI (*Numéro de Désignation de l'Installation*) : Partie de la numérotation téléphonique qui identifie l'installation privée.

NDIS (*Network Driver Interface Specification*) : Spécification Microsoft et 3-COM d'un logiciel permettant de piloter une carte d'interface réseau en s'affranchissant du protocole et des matériels utilisés. NDIS autorise l'utilisation simultanée de plusieurs protocoles réseaux sur le même adaptateur physique. Voir *ODI*.

NDS (*Numéro de Désignation Supplémentaire*) : Partie de la numérotation téléphonique qui désigne l'abonné.

NetBEUI (*Network Bios Extended User Interface*) : Interface de transport de la couche NetBIOS

NetBIOS (*Network Basic Input/Output System*) : Interface de couche Session pour réseaux de type IBM PC et Microsoft.

Newsgoups (*Usenet newsgroups*) : Forum de discussion thématique sur Internet.

NFS (*Network File System*) : Ensemble de protocoles développés par Sun Microsystems pour permettre l'accès partagé des fichiers sur un réseau. Parmi les suites « NFS » figurent notamment NFS, XDR (*External Data Representation*) et RPC (*Remote Procedure Call*) qui font partie d'une architecture plus importante que Sun appelle *ONC* (*Open Network Computing*)

NIC (*Network Interface Controller ou Network Interface Card*) : Voir *Adaptateur*.

NLPID (*Network Level Protocol Identifier*) : Elément d'information de l'encapsulation

définit par la RFC 1490 qui identifie le protocole transporté.

NNI (*Network Node Interface*) : Interface standard entre des commutateurs ATM. Également *Network-to-Network Interface* en relayage de trames. Dans un réseau SMDS, un NNI est appelé ISSI (*Inter-Switching System interface*).

Nœud : Terme générique utilisé pour faire référence à une entité pouvant accéder à un réseau. Synonyme de *station*. Système constituant un carrefour de lignes de communications dans un réseau : serveur, concentrateur, frontal.

Non-Répudiation : Mécanisme d'authentification dans lequel l'auteur d'un message ne peut nier l'avoir émis ou le destinataire l'avoir reçu.

Norme : Ensemble de règles ou de procédures consacrées par la pratique ou la décision d'un organisme officiel.

NSAP (*Network Service Access Point*) : Adresses réseau ISO, spécifiées par la norme ISO 8348/Ad. Point auquel les services réseaux OSI sont mis à la disposition d'une entité de transport.

Null modem : Voir *Éliminateur de modem*.

Numeris : Nom commercial du Réseau Numérique à Intégration de Services commercialisé par France Télécom. Voir *RNIS*.

Numérotation : Système de signalisation des adresses d'abonné (numéro d'abonné) dans un réseau téléphonique (plan de numérotation). Il existe deux types de numérotation : la numérotation décimale et la numérotation à fréquence vocale. Le plan de numérotation international est défini par la norme E.164.

Numérotation à fréquence vocale : Voir *Numérotation fréquentielle*.

Numérotation décimale ou analogique (33/66) : Numérotation téléphonique des postes téléphoniques à cadran. La numérotation est réalisée par ouverture de la liaison d'abonné. Les numéros sont envoyés au commutateur de rattachement sous forme d'impulsions de 66 ms suivi d'un repos de 33 ms, d'où le nom de système 33/66. Il est envoyé une impulsion pour le 1, deux pour le 2, etc.

Numérotation fréquentielle ou vocale : (multifréquentielle), Numérotation téléphonique normalisée (Q.23). Ce type de numéro est composé à partir du clavier à touche de téléphone. L'enfoncement d'une touche correspond à l'envoi de deux fréquences (la haute suivie de la basse) au central de rattachement (**DTMF**, *Dual-Tone MultiFrequency*). Les postes peuvent comporter 12 ou 16 touches. Certains postes téléphoniques fréquentiels ont la possibilité d'émettre une numérotation décimale. Transmise en transparence durant une conversation la numérotation à fréquence vocale autorise un dialogue homme machine.

Numérotation numérique ou binaire : Numérotation téléphonique des postes téléphoniques numériques. Ces postes émettent directement un signal binaire sur une voie dite de signalisation. La numérotation peut être propriétaire (poste numérique propriétaire) ou normalisée (RNIS).

NVL (*Numéro de Voie Logique*) : Étiquette d'identification d'une communication dans les réseaux X.25. Le NVL n'a qu'une valeur locale entre deux nœuds adjacents du réseau.

Nyquist (**Critère**) : Voir *Critère de Nyquist*.

O

Objet géré : En gestion de réseau, station qui peut être gérée par un protocole de gestion de réseau.

OCR (*Optical Character Recognition*) : Système de reconnaissance optique de caractères convertissant un document imprimé en un document texte.

© Dunod – La photocopie non autorisée est un délit

Octet : Terme générique utilisé pour faire référence à une série de 8 bits consécutifs traités comme un tout. Synonyme *Byte*.

ODI (*Open Data-link interface*) : Spécification Novell d'un progiciel pour cartes d'interface réseau. Voir *NDIS*.

ODIF (*Office Document Interchange Format*) : Format d'échange de documents dans le cadre de la norme ODA.

OEM *(Original Equipement Manufacturer)* : Constructeur ou distributeur qui revend un matériel ou un logiciel sous sa propre marque.

Opérateur de télécommunications : Organisation publique ou privée offrant des services de télécommunication.

OSI (*Open System Interconnection*) : Voir *Modèle OSI*.

OSPF (*Open Shortest Path First*) : Algorithme de routage IGP (*Interior Gateway Protocol*) hiérarchique à état des liaisons successeur de RIP dans le monde Internet. Ces fonctionnalités comprennent le routage à moindre coût, le routage multivoie et l'équilibrage des charges. L'OSPF est dérivé d'une ancienne version du protocole IS-IS de l'OSI. Voir *Algorithme de routage à état des liaisons.*

OUI (*Organization Unit Identifier*) : Premier champ de l'adresse MAC IEEE. OUI identifie le manufacturier de l'interface réseau.

Outsourcing : Voir *Facilities Managment*.

P

PABX (*Private Automatic Branch eXchange*) : Voir *Autocommutateur privé*.

Packet : Voir *Paquet*.

Packets switching : Voir *Commutation de paquets.*

PAD (*Packet Assembler-Disassembler*) : Il a pour objectif essentiel d'encapsuler les données issues du terminal asynchrone (ETTD-C) dans un paquet X.25 et de décapsuler les données à destination de ce terminal. Afin d'éviter que sur le réseau ne circule un paquet pour chaque caractère, le PAD assemble ces caractères en paquets. L'avis X.3 précise les modalités essentielles de cette fonction.

Paire torsadée : Support de transmission composé de deux fils isolés disposés selon une configuration en spirales régulières. Les fils peuvent être blindés ou non blindés. La paire torsadée est très courante dans les applications téléphoniques, et de plus en plus utilisée dans les réseaux locaux.

PAM (*Pulse Amplitude Modulation*) : Voir *Modulation d'impulsions en amplitude*.

PAN (*Personnal Area Network*) : Système de transmission de données à usage personnel. Voir *Bluetooth*.

PAP (*Password Authentification Protocol*) : Sous protocole d'authentification par échange de mot de passe de PPP (*Point to Point Protocole*).

Paquet (*Packet*) : Unité de données du niveau 3 du modèle OSI. Voir aussi *Trame*, *Datagramme*, *Segment* et *Message.*

Paradiaphonie : La paradiaphonie exprime l'affaiblissement du signal reçu sur une paire par rapport au signal transmis sur une autre paire. Plus la valeur est élevée meilleur est le câble.

Pare-feu : Équipement réseau de sécurité qui effectue un filtrage des données. Synonyme *Firewall*.

Parité : Voir *Contrôle de parité*.

Passerelle (*Gateway*) : Élément d'interconnexion de réseau de niveau supérieur à 3. Les passerelles applicatives sont très utilisées pour permettre l'interfonctionnement de programmes aux fonctionnalités identiques mais fonctionnant sur des systèmes incompatibles (exemple passerelle de messagerie). Ce terme a longtemps été utilisé dans le monde TCP/IP pour désigner des routeurs (Passerelles interréseau).

Payload : Correspond au champ de données d'une unité de données. Synonyme *charge utile*.

PBX (*Private Branch eXchange*) : Voir *Autocommutateur privé*.

PCI (*Protocol Control information*) : Informations de contrôle ajoutées aux données de l'utilisateur pour composer un paquet OSI. Équivalent OSI du terme *En-tête*.

PCM (*Pulse Code Modulation*) : Voir *MIC*.

PDH (*Plesiochronous Digital Hierarchy*) : Hiérarchie de multiplexage temporel qui regroupe au premier niveau 32 IT (2 048 kbit/s) en Europe (E1) et 24 IT en Amérique du Nord et au Japon (T1).

PDU (*Protocol Data Unit*) : Unité de données échangées entre des stations à un niveau spécifique du modèle OSI.

Peer to Peer : Voir *Égal à égal*.

Périphérique : Entité pouvant accéder à un réseau. Synonyme de *Nœud.*

PgP (*Pretty Good Privacy*) : Logiciel de cryptographie utilisé pour les échanges sur Internet.

Phase : Un des trois éléments définissant une onde, avec son amplitude et sa fréquence.

Piggyback : Procédure selon laquelle l'accusé de réception d'un bloc de données est inséré dans un bloc de données émis sur une liaison duplex. Cette procédure optimise le débit global.

PIH (*Protocol Identifier Header*) : Champ de l'encapsulation SNAP (*SubNetwork Access Protocol*) qui identifie le protocole transporté.

Pile de protocoles : Ensemble des couches de logiciels dont l'interaction permet de réaliser une architecture de communication. Synonyme *Stack*.

PIN (*Personnal Identification Number*) : Code personnel d'authentification utilisé en GSM.

Ping (*Packet INternet Groper*) : Message d'écho ICMP et sa réponse, souvent utilisés pour tester l'accessibilité d'une station du réseau.

Pipe : Processus qui permet la communication directe entre deux programmes que ceux-ci soient locaux ou distants. La sortie du flux d'information de l'un correspond à l'entrée de l'autre.

Pixel (*Picture Element*) : Point élémentaire d'une image numérique.

Plésiochrone : Caractéristique d'un réseau numérique synchronisé dans lequel chacune des stations communicantes est synchronisée sur une source d'horloge différente mais de fréquences et de stabilité identiques.

PLP (*Packet Level Protocol*) : Autre désignation du protocole X.25. Voir *X.25*.

Point à point : Caractéristique d'une liaison ne connectant que deux équipements. Inverse de *multipoint*.

Polling : Technique de scrutation d'un terminal. Voir *Invitation à émettre*, *Appel sélectif*.

Pont : Unité fonctionnelle qui interconnecte deux segments de réseaux, et permet le transfert de paquets entre eux. Le pont agit au niveau 2 (Liaison de données) du modèle OSI et est indépendant des protocoles des couches supérieures. Dans les environnements locaux les ponts ont été remplacés par des commutateurs. Ces derniers offrent les mêmes fonctionnalités mais assurent une transmission plus rapide.

Pont distant : Pont qui relie des segments de réseaux physiquement distincts par des liaisons WAN.

Pont local : Pont qui relie directement des réseaux d'une même région géographique.

Pont-routeur : Voir *B-Router*.

Pontage transparent : Système de pontage adopté par les réseaux Ethernet et IEEE 802.3 selon lequel des ponts transmettent des trames saut par saut en fonction de tables

© Dunod – La photocopie non autorisée est un délit

associant des nœuds d'extrémité (adresse MAC) à des ports de ponts.

Port : Interface physique entre une ligne et un équipement de réseau (routeur, par exemple). En terminologie IP, terme également utilisé pour spécifier le processus récepteur de la couche supérieure.

Porteuse (*Carrier signal*) : Tonalité ou signal radio modulé par des données à transmettre.

POTS (*Plain Old Telephone Service*) : Service standard de téléphone analogique fréquemment utilisé aux États-Unis.

PPP (*Point-to-Point Protocol*) : Protocole dérivé d'HDLC, successeur de SLIP qui offre des connexions de routeur à routeur et d'hôte à réseau sur des circuits synchrones et asynchrones. Voir aussi *SLIP*.

PRI (*Primaty Rate Interface*) : Interface RNIS à accès primaire. Cet accès se compose d'un unique canal D à 64 kbit/s et de 23 (aux USA accès T1 à 1,544 Mbit/s) ou de 30 (en Europe accès T2 à 2,048 Mbit/s) canaux B pour la voie et/ou les données. Voir aussi *RNIS large bande et RNIS*.

Private Automatic Branch Exchange : Voir *Autocommutateur privé*.

Protocole : Description formelle de règles et de conventions régissant la manière dont les stations d'un réseau échangent des informations.

Protocole de routage : Protocole d'échange d'information de routage et d'établissement des tables de routage. Exemples de protocole de routage : IGRP, RIP et OSPF.

Protocole orienté bit : Type de protocole de transmission sur couche Liaison de données qui peut transmettre des trames quel que soit leur contenu. Comparés aux protocoles niveau octet, les protocoles niveau bit sont plus efficaces et plus fiables, et permettent de fonctionner en duplex.

Protocole point-à-point : Voir *PPP*.

Proxy (synonyme de *mandataire*) : Technique dans laquelle une machine ou un logiciel répond aux requêtes en lieu et place d'une ou plusieurs machines. Le proxy peut ainsi réaliser des opérations que le programme d'origine n'aurait pu effectuer (incompatibilité ou autre).

PSDN (*Packet Switched Data Network*) : Réseau de transmission utilisant la commutation de paquets. Désigne généralement un réseau X.25.

PSK (*Phase Shift Keying*) : Voir *Modulation de phase*.

PSN (*Packet Switch Node*) : Nœud de commutation de paquets. Généralement le PSN est un ETCD qui permet la connexion à un ETTD. Voir aussi *X.25*. Cet acronyme est également couramment utilisé pour *Packet Switch Network*.

Puissance lexicographique : On appelle puissance lexicographique d'un code le nombre de symboles qu'il est possible de représenter à l'aide de ce code. En logique binaire avec n éléments binaires on peut représenter 2^n symboles (code à n moments).

PVC (*Permanent Virtuel Circuit*) : Voir *Circuit virtuel permanent*.

Q

Q.920/Q.921 : Avis du CCITT pour les interfaces réseau-utilisateurs RNIS portant sur la Couche 2 du modèle ISO. Voir aussi *UNI*.

Q.931 : Avis du CCITT, standard de signalisation des connexions RNIS.

Q-SIG (*Signalisation au point Q*) : Norme de signalisation développée par l'ECMA et normalisé par l'ISO pour permettre un dialogue entre PABX hétérogènes.

Q.932 : Avis du CCITT qui constitue le standard de la signalisation de l'établissement des circuits virtuels ATM et une évolution de l'avis CCITT Q.931.

QoS (*Quality of Service*) : Voir *Qualité de service*.

Qualité de service : Mesure des performances d'un système qui reflète sa qualité de transmission et la disponibilité du service.

R

Radio Cellulaire : Technique d'organisation des transmissions radiofréquences dans laquelle on établit une correspondance entre une fréquence et une zone géographique (Cellule). Cette organisation autorise le réemploi des fréquences dans des cellules non contiguës.

RAID (*Redundant Array of Inexpensive Disk*) : Système de disques à tolérance de panne.

Rapidité de modulation : Voir *Baud*.

RARP (*Reverse Address Resolution Protocol*) : Inverse logique de ARP qui permet à une station d'obtenir une adresse IP.

RAS (*Remote Access Service*) : Système de contrôle des accès distants.

Réassemblage : Reconstitution d'une unité de données après sa fragmentation par la source ou à un nœud intermédiaire.

Récupération des silences (DSI, *Digital Speech Interpolation*) : Lors d'une communication téléphonique environ 60 % du temps est inutilisé par la communication (silence). La technique de récupération des silences récupère ces instants pour effectuer des transmissions de données. Pour éviter que le correspondant distant n'ait l'impression que la communication est interrompue le DSI réinjecte, localement, du souffle.

Redirection : Partie des protocoles ICMP et ES-IS qui permet à un routeur d'indiquer à un hôte que l'utilisation d'un autre routeur serait plus efficace.

Région : Ensemble logique de sous-réseaux interconnectés et constituant un domaine de routage autonome.

Reject sélectif : Technique dans laquelle le récepteur ne demande la retransmission que du seul bloc reçu erroné. L'utilisation du rejet sélectif implique que le récepteur ait la capacité de mémorisation des blocs reçus ultérieurement à celui erroné et que le récepteur soit capable d'assurer le réordonnancement des blocs avant de les délivrer à la couche supérieure. Le nombre de blocs en attente s'appelle la fenêtre de réception. Voir *Rejet simple*.

Rejet simple : Technique dans laquelle le récepteur demande à l'émetteur de reprendre la transmission à partir du bloc reçu erroné. Le récepteur n'a aucune capacité de stockage ni de réordonnancement, la fenêtre de réception est de 1. Voir *Rejet sélectif*, *Fenêtre de réception*.

Relais : Terminologie OSI décrivant une unité qui connecte plusieurs réseaux ou systèmes de réseaux. Un relais de Couche 2 est un pont, et un relais de Couche 3, un routeur.

Relais de trame (*Frame Relay*) : Protocole réseau issu d'HDLC LAP-B et présenté comme une simplification d'X.25.

Remise pour le mieux *(Best Effort*) : Se dit des réseaux datagrammes dans lesquels aucune garantie de remise au destinataire n'est donnée.

RENATER : Réseau NAtional de TElécommunications de la Recherche.

Répéteur : Équipement qui régénère le signal d'information et le signal d'horloge. Un répéteur permet d'augmenter la portée d'un système de transmission.

Réseau cellulaire : Réseau de télécommunication spécialement destiné aux équipements mobiles et qui permet la communication entre ces unités mobiles, ainsi qu'avec l'ensemble des abonnés au téléphone du monde entier. Le territoire couvert est divisé en cellules, et chaque cellule est équipée d'une station fixe à laquelle est attribué un certain nombre de fréquences radio-électriques.

Réseau d'entreprise : Réseau (généralement important et diversifié) connectant les principaux points d'une entreprise. À la dif-

© Dunod – La photocopie non autorisée est un délit

férence du WAN, ce type de réseau est généralement privé, et ne concerne qu'une entreprise.

Réseau dorsal (*Backbone*) : Réseau jouant le rôle d'artère principale pour le trafic qui circule souvent en bidirectionnel, c'est-à-dire à la fois à destination et en provenance d'autres réseaux.

Réseau local (LAN, *Local Area Network*) : Réseau couvrant une surface géographique relativement peu étendue (généralement un étage ou un bâtiment). Comparés aux réseaux longue distance, les réseaux locaux ont généralement des débits de transmission élevés et des taux d'erreur faibles. Synonyme *réseau local d'entreprise*, ou *RLE*. Voir aussi *Réseau longue distance* (WAN) et *Réseau métropolitain* (MAN).

Réseau longue distance : Voir *WAN*.

Réseau métropolitain : Voir *MAN*.

Réseau privé : Voir *Réseau d'entreprise.*

Réseau privé virtuel : Ensemble de ressources de communication logiquement organisées par un service d'exploitation public et mise à la disposition du client de façon à apparaître – comme – son réseau privé.

Réservation de bande passante : Dans les réseaux commutés, processus permettant de réserver des ressources à une communication.

Résolution d'adresses : Méthode permettant de faire correspondre les adresses de niveau 3 OSI (couche Réseau) aux adresses MAC.

Résolution de nom : Association d'un nom à une adresse de réseau.

Résolution dynamique d'adresses : Utilisation d'un protocole de résolution d'adresses pour déterminer et stocker à la demande des informations sur les adresses.

RFC (*Request For Comments*) : Documents normatifs dans l'environnement TCP/IP. Certains RFC sont déclarés par l'AB « standard Internet ». La plupart des RFC concernent des spécifications de protocole comme Telnet et FTP, mais certains sont humoristiques et/ou historiques. Les RFC sont fournis par les Network Information Centers d'Internet.

RHM (*Relation Homme Machine*) : Terme désignant généralement le programme de gestion d'un système et par extension la console d'accès à ce système.

RIF (*Routing Information Field*) : Champ de l'en-tête IEEE 802.5 qui est utilisé par un pont pour déterminer les anneaux Token Ring par lesquels une trame MAC doit transiter. Le RIF comporte notamment un numéro de pont et un numéro d'anneau.

RIP (*Routing Information Protocol*) : Protocole de routage entre passerelles fourni avec les systèmes UNIX Berkeley. L'IGP le plus répandu dans l'internet. Le protocole RIP utilise le *nombre* de *sauts* comme métrique de routage. Le nombre maximum de sauts autorisés pour ce protocole est fixé à 16.

RJ-45 : Connecteur glissant à 8 fils utilisé dans les réseaux locaux (IEEE 802.3 1 base 5 ou StarLAN et 10 base T). Également utilisé dans certains cas pour les lignes téléphoniques (RNIS).

RLE : Réseau Local d'Entreprise Voir *Réseau local*.

RMON (*Remote MonitOr Network*) : Sonde destinée à remonter des informations d'administration.

RNIS (*Réseau Numérique à Intégration de Services*) : Ensemble de protocoles de communication proposé par les opérateurs de téléphone pour transporter, sur une même infrastructure, plusieurs services concernant la voix, les données ou les images. Ce réseau permet de connecter des équipements téléphoniques (autocommutateurs), des équipements informatiques (terminaux), la téléco-

pie et le vidéotex. Voir aussi *RNIS large bande*.

RNIS large bande : Norme de transmission développée par le CCITT (UIT-T) pour transmettre des applications nécessitant une bande passante importante comme la vidéo. Ce standard utilisera la technologie ATM sur des circuits de transmission SONET pour offrir des vitesses de transfert de données comprises entre 155 Mbit/s et 622 Mbit/s, et au-delà. Voir aussi *RI, RIS et PRI*.

Roaming ou **itinérance** : Fonction de localisation dans un système de radiocommunication avec les mobiles.

RON/TRON (*RéceptiON/TRansmissiON*) : Voir *E&M*.

Routage : Processus de détermination du chemin d'accès vers un hôte distant. Dans les réseaux importants, ce processus est très complexe en raison du nombre de destinations intermédiaires potentielles qu'un paquet peut traverser avant d'atteindre sa destination.

Routage adaptatif : Voir *Routage dynamique*.

Routage de plus court chemin : Routage qui réduit au minimum les coûts de transmission par application d'un algorithme approprié.

Routage de type de service : Système de routage dans lequel le choix d'une voie du réseau dépend des caractéristiques des sous-réseaux concernés, du paquet et du plus court chemin entre le point considéré et sa destination.

Routage dynamique : Routage qui s'ajuste automatiquement à la topologie ou à la charge du réseau. Synonyme *Routage adaptatif*.

Routage hiérarchique : Routage basé sur un système d'adressage hiérarchique. Par exemple, les algorithmes de routage IP utilisent des adresses IP, qui contiennent des numéros de réseaux, des numéros d'hôtes et (éventuellement) des numéros de sous-réseaux.

Route : Synonyme de *Chemin*.

Route par défaut : Entrée d'une table de routage qui est utilisée pour diriger des trames pour lesquelles un saut suivant n'est pas explicitement mentionné dans la table de routage.

Route statique : Route qui est entrée manuellement dans la table de routage par défaut. Les routes statiques ont priorité sur toutes les routes choisies par tous les protocoles de routage dynamique.

Routeur : Système relais de niveau 3 qui permet de choisir, parmi plusieurs chemins, celui que suivra le trafic du réseau en fonction d'une métrique optimale. (Également appelé *passerelle*, dans l'environnement TCP/IP, bien que ce terme de passerelle soit de moins en moins utilisé) le routeur transmet des paquets d'un réseau à un autre, en fonction d'informations de couche de réseau.

Routeur désigné : Routeur OSPF qui génère une annonce d'état de liaison pour un réseau multiaccès et a d'autres responsabilités dans le déroulement du protocole. En OSPF, chaque réseau multiaccès ayant au moins deux routeurs connectés a un routeur désigné. Celui-ci, choisi par le protocole Hello OSPF, permet de réduire le nombre de contiguïtés nécessaires dans un réseau multiaccès. Ceci diminue également le trafic des protocoles de routage et la taille de la base de données topologique.

Routeurs voisins : En OSPF, deux routeurs qui ont des interfaces avec un réseau commun. Dans les réseaux multiaccès, les voisins sont découverts dynamiquement par le protocole Hello de l'OSPF.

RPC (*Remote Procedure Call*) : Voir *Appel de procédure à distance.*

RPIS (*Réseau Privé à Intégration de Services*) : Réseau privé de type RNIS autori-

© Dunod – La photocopie non autorisée est un délit

sant le transfert de la voix, des données et de l'image.

RPV (*Réseau Privé Virtuel*) : Voir *VPN*.

RS-232C : Interface de couche physique, pratiquement identique à l'avis V.24.

RSA (*River Shamir et Adelman*) : Algorithme de chiffrement à clés publiques et clés secrètes portant le nom de ses concepteurs.

RSVP (*Ressource ReSerVation Protocol*) : Protocol de signalisation de l'environnement TCP/IP qui consiste pour un flux IP donné à « baliser » un chemin en y réservant des ressources.

RTC (*Réseau Téléphonique Commuté*) : Réseau utilisé pour le téléphone classique.

RTT (*Round-Trip Time*) : Voir *Temps de transmission aller-retour*.

S

SAR (*Segmentation and Reassembly*) : Voir *Segmentation et réassemblage*.

Saut : Passage d'un routeur au routeur suivant (hop).

SDA (*Sélection Directe à l'Arrivée*) : Service téléphonique permettant de joindre directement le poste demandé sans passer par le standard de l'entreprise. La SDA est un service, le nombre de numéros SDA attribué n'est pas lié au nombre de lignes de l'abonnement, mais au nombre de postes téléphoniques connectés au PABX local.

SDH (*Synchronous Digital Hierarchy*) : Hiérarchie numérique synchrone destinée aux infrastructures des grands réseaux de télécommunication. Grâce à une technique de distribution des horloges à tous les niveaux de concentration, le SDH autorise une gigue faible. Voir *PDH*

SDLC (*Synchronous Data Link Control*) : Protocole IBM de couche de liaison de données orienté bit, qui a donné naissance à de nombreux protocoles similaires dont HDLC et LAP-B.

SDU (*Service Data Unit*) : Unité de données du modèle OSI à la limite entre deux couches.

SECAM (*Sequentiel Couleur A Mémoire*) : Système de télévison couleur français dans lequel l'information concernant une couleur est envoyée une ligne sur deux et mise en mémoire pour en disposer la ligne suivante.

Segment : Terme utilisé en spécification TCP pour décrire une unique unité d'information de couche transport. Voir *Message*.

Segmentation : Opération qui consiste à découper une unité de données en unités plus petites lors d'une transmission sur un support de réseau qui ne peut pas supporter la taille d'origine de l'unité de données.

Segmentation et réassemblage : Processus par lequel les unités de données sont segmentées en cellules ATM à l'émission et réassemblées sous le format d'origine à la réception.

Selecting : Technique de scrutation d'un terminal. Voir *Invitation à recevoir*.

Sémaphore : Indicateur d'état dans un processus. Voir aussi *Canal Sémaphore*

Semi-duplex : Voir *Half-duplex*.

Série de Fourier : Voir *Théorème de Fourier*.

Serveur de noms : Serveur du réseau qui associe un nom de machine à son adresse réseau.

Serveur Web : Système hébergeant des documents hypertextes mis à disposition sur Internet ou en Intranet et consultable par un logiciel de navigation.

Signal analogique : Signal électrique variant de manière analogue à un phénomène physique (voix, pression...). Les signaux analogiques sont essentiellement caractérisés par l'infinité de valeurs prises par le signal entre les bornes de variation du phénomène physique.

Signalisation E&M : Standard de signalisation téléphonique utilisée sur les lignes interurbaines et intercommutateurs. Voir *RON/TRON*.

Signalisation hors bande : Code de transmission utilisant des fréquences ou des canaux situés en dehors des fréquences ou des canaux utilisés normalement pour le transfert d'informations. Cette méthode est souvent utilisée pour la signalisation des erreurs lorsque la signalisation intra-bande peut être affectée par les problèmes qui peuvent se poser sur le réseau.

Signalisation intrabande : Transmission d'information de service sur le même canal que celui utilisé pout la transmission des données. À l'opposé, la signalisation hors-bande qui utilise pour les informations de service un canal dédié différent du canal de transmission des données.

Signalisation par canal sémaphore : Système de signalisation hors bande utilisé par de nombreux réseaux téléphoniques, qui sépare les informations de signalisation des données utilisateur.

Signalisation : Processus qui consiste à envoyer un signal de transmission sur un support physique pour établir une communication.

SIM (*Subscriber Identification Module*) : Carte à puce utilisée dans un système terminal GSM et qui contient toutes les informations relatives à l'abonné.

SIMlock : Verrouillage, par l'opérateur, de la carte SIM, pour en interdire l'usage.

SLIP (*Serial Line Internet Protocol*) : Protocole utilisé pour transporter IP sur des liaisons séries (circuits téléphoniques par exemple). SLIP n'assure que la délimitation des unités de données (datagrammes IP).

SMDS (*Switch Multimegabit Data Service*) : Service de transfert rapide de données (organisé en cellules de taille fixe) sur longue distance, défini par les laboratoires américains BelCore. Achemine du trafic issu des réseaux locaux : Synonyme *CBDS*.

SMS (*Short Message Service*) : Service d'envoi de messages courts à destination d'un téléphone mobile.

SMTP (*Simple Mail Transfer Protocol*) : Protocole internet offrant des services de courrier électronique.

SNA (*System Network Architecture*) : Architecture générale de communications en couches développée par IBM au cours des années soixante-dix.

SNMP (*Simple Network Management Protocol*) : Protocole de gestion des réseaux Internet qui permet de contrôler et de spécifier la configuration du réseau et les paramètres d'exécution.

SNPA (*SubNerwork Point of Attachment*) : Adresse d'un point d'accès au réseau de transport. Une adresse X.121 désigne un SNPA.

Socket : Structure logicielle fonctionnant comme point d'accès entre couches de communication dans une station en réseau (API socket).

Somme de contrôle : Méthode permettant de vérifier l'intégrité des données transmises. Une somme de contrôle est une valeur entière calculée par une série d'opérations arithmétiques sur une séquence d'octets. La valeur est recalculée à l'extrémité réceptrice et comparée à la valeur d'origine. Voir *Checksum*, *CRC*, *FCS*.

SONET (*Synchronous Optical Network*) : Réseau synchrone rapide (pouvant fonctionner à 2,5 Gbit/s) déclaré norme internationale en 1988. Voir *SDH*.

Source routing : Technique de routage dans laquelle c'est l'émetteur du message qui définit la route à suivre Les données sont émises avec la liste des nœuds à traverser.

© Dunod – La photocopie non autorisée est un délit

Sous-canal : En terminologie large bande, subdivision de fréquences créant un canal de communications séparé.

Sous-couche MAC (MAC, *Medium Access Control*) : Voir *MAC*.

Sous-réseau : Terme parfois utilisé pour faire référence à un segment de réseau. Dans les réseaux IP, sous-ensemble de machines réseau partageant une adresse réseau particulière et distingué par un champ de bits (SubNet_ID).

Spanning tree : Voir *Algorithme du spanning tree*.

Spectre de fréquences : Voir *Largeur de bande*.

SPOOL (*Simultaneous Peripherals Operation On-Line*) : Voir *Spooler.*

Spooler : Application qui gère les requêtes ou les travaux qui lui sont soumis à des fins d'exécution. Les spoolers traitent les requêtes qui lui sont soumises dans l'ordre dans lequel elles figurent dans la file d'attente. L'exemple le plus connu de spooler est probablement le spooler d'impression.

SQE (*Signal Quality Error*) : Dans les réseaux Ethernet, message renvoyé par un récepteur au contrôleur pour lui indiquer si le circuit de collision fonctionne.

SQL (*Structured Query Langage*) : Langage de requêtes pour base de données développé par IBM.

STA (**Spanning Tree Algorithm**) : Voir *Algorithme du spanning tree*.

Standard de fait : Standard consacré davantage par l'usage que par un décret officiel. Standard par défaut.

Station primaire : Dans les protocoles de couche Liaison de données synchrone par bit comme HDLC et SDLC, station qui contrôle la transmission des stations secondaires et assure d'autres fonctions de gestion comme le contrôle des erreurs (par rejet sélectif ou autre). Les stations primaires envoient des commandes aux stations secondaires et en reçoivent des réponses. Voir aussi *Station secondaire*.

Station secondaire : Dans les protocoles de couche de liaison de données synchrone orientés bit, comme HDLC, station qui réagit aux commandes que lui envoie une station primaire. Voir aussi S*tation primaire*.

Store and forward : Technique de commutation de messages dans laquelle des messages sont stockés momentanément en des points intermédiaires entre la source et la destination, jusqu'à ce que les ressources du réseau (une liaison non utilisée, par exemple) soient disponibles.

STP (*Shielded Twisted Pairs*) : Paire torsadée blindée. Câble constitué de plusieurs paires torsadées protégées par un blindage.

Suppresseur d'écho : Dispositif utilisé pour éliminer les échos sur les transmissions vocales à longue distance. L'écho provient généralement d'une désadaptation d'impédance au passage de la ligne de 2 à 4 fils et inversement.

SVC (*Switch Virtual Circuit*) : Voir *Circuit virtuel commuté*.

Switched Ethernet : Voir *Commutation Ethernet*.

Synchrone : Caractéristique d'un mode de transmission dans lequel l'émetteur et le récepteur fonctionnent au même rythme, calés sur une même horloge.

Syntaxe abstraite : Description de structure de données indépendante des structures et des codes matériels (exemple ASN-1).

Système à tolérance de pannes (SFT, *System Fault Tolerance*) : Ensemble de mécanismes mis en œuvre pour pallier la défaillance d'un élément du système et assurer la continuité du service. Les principaux mécanismes mis en œuvre dans les systèmes à tolérance de pannes sont : les disques miroirs, les disques en duplex.

Système autonome : Ensemble de réseaux ayant une administration commune et une stratégie de routage commune. Un système autonome doit avoir un numéro d'identification à 16 bits qui lui est affecté par le centre d'information réseaux (également appelé NIC ou *Network Information Center*).

Système intermédiaire : Voir *Relais*.

T

T0 : Voir *Accès de base.*

T1 : Accès spécifique, non disponible en France, du réseau RNIS faisant référence à lien multiplex numérique utilisé pour la transmission des données à 1,544 Mbit/s sur lignes téléphoniques.

T2 : Voir *Accès primaire.*

TAPI (*Telephony Application Programming Interface*) : Ensemble de DLL de Microsoft permettant le développement d'applications de gestion des communications téléphoniques. Voir *TSAPI*.

TCP/IP (*Transmission Control Protocol/Internet Protocol*) : Regroupement de deux protocoles Internet bien connus, souvent considéré à tort comme un seul et même protocole. TCP correspond à la couche 4 (Transport du modèle OSI) et permet une transmission fiable des données. IP correspond à la couche 3 (couche réseau du modèle OSI) et offre un service de datagrammes en mode non connecté. TCP/IP a été développé pour le ministère américain de la défense dans les années soixante-dix.

TDM (*Time Division Multiplexing*) : Voir *Multiplexage à répartition temporelle*.

TDMA (*Time Division Multiple Access*) : Voir *AMRT*

TEI (*Terminal End-Point Identifier*) : Champ de la trame LAP-D sur 7 bits, qui correspond à l'identification du terminal proprement dit. Les TEI peuvent être attribués par le constructeur (TEI de 0 à 63) ou par le réseau, la TNR alloue les TEI de 64 à 126. Le TEI 127 est réservé à la diffusion de messages. Lorsqu'un terminal à allocation automatique de TEI est connecté au bus, il demande au réseau de lui attribuer un TEI. Alors qu'un terminal à affectation non automatique s'assure de l'unicité de son TEI. Un terminal multifonctions peut utiliser plusieurs TEI, un par fonction.

Télécommunications : Terme regroupant l'ensemble des techniques de transmission.

Télécopieur : Système de transmission de l'écrit par numérisation du document et transmission. Le résultat de la transmission est une télécopie ou fac similé.

Tempête de diffusion : Phénomène survenant sur le réseau lorsque plusieurs messages sont transmis simultanément, en utilisant une largeur de bande importante.

Temporisation (retransmission sur temporisation) : Événement qui se produit lorsqu'une station d'un réseau s'attend à recevoir d'une autre station du réseau des informations qui ne lui parviennent pas pendant le délai prévu. La temporisation entraîne généralement une retransmission des informations ou l'annulation du circuit virtuel entre les deux stations.

Temps de groupe : Voir *Distorsion de phase*.

Temps de propagation : Voir *Délai de propagation*.

Temps de transmission aller-retour (RTT, *Round-Trip Time*) : Temps compris entre le moment d'émission d'un message et la réception de son accusé de réception. Le RTT est utilisé dans certains algorithmes de routage pour le calcul des routes optimales.

Terminaison : Résistance électrique placée à l'extrémité d'une ligne de transmission, et qui absorbe les signaux circulant sur la ligne, empêchant ainsi l'écho.

Terminal asynchrone : Terminal très simple dans lequel chaque caractère entré au cla-

© Dunod – La photocopie non autorisée est un délit

vier est immédiatement transmis au système hôte. Le système hôte renvoie au terminal le caractère reçu qui est alors affiché (écho distant). Certains terminaux asynchrones gèrent l'écho localement. Les terminaux Minitel, VT100 et Telnet sont des exemples de terminaux asynchrones. Les caractères sont envoyés sur le support au rythme de la frappe, la transmission est du type asynchrone. Voir *Asynchrone, Terminal synchrone*.

Terminal synchrone : Terminal dans lequel les caractères frappés au clavier ne sont transmis qu'après validation (par bloc). L'écho des caractères introduit est local. La transmission entre le terminal et le système hôte est dite transmission synchrone. Voir *Synchrone, Terminal asynchrone*.

TFTP (*Trivial File Transfer Protocol*) : Version simplifiée de FTP qui permet le transfert de fichiers d'un ordinateur à l'autre sur un réseau.

Théorème de Fourier : Une fonction périodique de fréquence f_o peut être considérée comme la somme d'une constante (*composante continue*) et de fonctions sinusoïdales de fréquence égale à celle du signal périodique (*fondamental*) et multiple de celle-ci (*harmoniques*). Est utilisée notamment pour passer du domaine temporel au domaine fréquentiel dans l'analyse des signaux, c'est-à-dire pour transformer une impulsion en une somme de signaux périodiques sinusoïdaux afin d'étudier le comportement d'un système auquel on applique ce signal.

Théorème de Shannon : Le théorème de Shannon définit la fréquence minimale d'échantillonnage d'un signal. Celle-ci doit être au minimum le double de la fréquence maximale du signal à échantillonner

Time Out : Exprime la borne maximale pour qu'un événement intervienne. Voir *Temporisation*.

Time slot : Voir *IT*.

Token Ring : Réseau local à passage de jeton développé et supporté par IBM. Très semblable à un réseau local (LAN) IEEE 802-5.

Topologie : Disposition physique des nœuds et des supports d'un réseau dans une structure de réseaux d'entreprise.

Topologie en anneau : Topologie dans laquelle le réseau se compose d'une série de répéteurs reliés les uns aux autres par des liaisons de transmission unidirectionnelle pour former une unique boucle fermée. Chaque station du réseau se connecte au réseau au niveau d'un répéteur.

Topologie en bus : Architecture LAN selon laquelle les transmissions des stations du réseau se propagent sur toute la longueur du support et sont reçues par toutes les autres stations.

Topologie en étoile : Topologie dans laquelle les extrémités d'un réseau sont connectées à un commutateur central commun par des liaisons point à point.

Topologie logique : Topologie qui caractérise le dialogue dans un réseau local. Voir *Topologie physique*.

Topologie physique : Désigne comment les stations d'un réseau local sont raccordées au réseau, alors que le topologie logique caractérise l'échange de messages. Le réseau Token Ring a une topologie physique en étoile (les stations sont raccordées à un concentrateur spécifique, le MAU) alors que l'échange des messages s'effectue selon un anneau (topologie logique en anneau).

Total de contrôle : Voir *Somme de contrôle*.

TP4 (*Transport Protocol Class 4*) : Protocole de transfert ISO en mode connecté défini par la norme ISO 8073.

Trame : Groupe logique d'informations supporté et transmis par la couche Liaison de données. Les termes *paquet*, *datagramme*, *segment* et *message* sont également utilisés pour décrire des groupes d'information

logique à différentes couches du modèle ISO et dans différents cercles technologiques.

Tranceiver : Voir *MAU*.

Transmetteur : Voir *MAU*.

Transmission analogique : Technique de transmission de signaux selon laquelle l'information est transmise par variation d'une combinaison d'amplitude, de fréquence et de phase de signaux.

Transmission asynchrone : Mode de transmission dans lequel les horloges émission et réception sont indépendantes. Les caractères sont entre des bits de contrôle appelés *bits de départ et bits d'arrêt* (ou *start* et *stop*), qui désignent le début et la fin des caractères.

Transmission isochrone : Transmission asynchrone (start-stop) sur liaison de données synchrone. En téléphonie, le terme isochrone implique un échantillonnage constant du débit, et est considéré comme l'inverse de la transmission asynchrone.

Transmission parallèle : Transmission simultanée de tous les bits composant un caractère ou un octet. Voir aussi *Transmission série*.

Transmission série : Méthode de transmission des données dans laquelle les bits d'un caractère de donnée sont transmis de manière séquentielle sur un unique canal. Voir aussi *Transmission parallèle*.

Transmission synchrone : Mode de transmission dans lequel l'émetteur et le récepteur fonctionnent au même rythme, calés sur une même horloge.

Trap : Message non sollicité envoyé par un agent SNMP à un système de gestion de réseau (NMS) pour signaler l'apparition d'un événement significatif.

Trou noir : Terme de routage appliqué à une zone d'interconnexion de réseau dans laquelle les paquets entrent, mais d'où ils ne sortent pas, en raison de l'existence de conditions défavorables ou d'un problème de configuration de systèmes sur une partie du réseau.

Trunk : Canal formé par plusieurs lignes de base reliant deux autocommutateurs.

Tube cathodique (*CRT, Cathode Ray Tube*) : Élément de visualisation de la console écran.

Tunnel : Voir *Encapsulation*

Tunneling : Voir *Encapsulation*.

U

UART (*Universal Asynchronous Receiver and Transmitter*) : Composant électronique émettant ou recevant des caractères sur une ligne de transmission en mode série asynchrone.

UBR (*Unspecified Bit Rate*) : Classe de service dans ATM dans laquelle aucune garantie de qualité de service n'est donnée à la source. Mode *Best Effort*. Voir *ABR, CBR, VBR.*

UDP (*User Datagram Protocol*) : Protocole de couche Transport sans connexion appartenant à la famille des protocoles Internet.

UIT (*Union Internationale de Télécommunications*) : Organisme international dont le siège est à Genève et qui est chargé, dans le cadre de l'ONU, des questions de télécommunications.

UMTS (*Universal Mobile Telecommunications System*) : Système de téléphonie mobile autorisant des accès hauts débits à Internet.

UNI (*User Network Interface*) : Interface réseau utilisateur définie par le forum ATM pour l'accès aux réseaux ATM privés et publics.

Unicast : Voir *Adresse à diffusion unique.*

URAD (Unité de Raccordement d'Abonnés Déportés) : Élément d'une installation de téléphonie qui autorise le raccordement d'abonnés ne pouvant être raccordés directement à l'installation principale. L'URAD et

© Dunod – La photocopie non autorisée est un délit

le PABX principal peuvent être reliés par des LIA ou par un lien MIC.

URL (*Uniform Ressource Locator*) : Adresse logique d'un système dans le réseau Internet.

UTP (*Unshielded Twisted Pairs*) : Câble à paires torsadées non écranté. Les câbles UTP représentent la majorité des câblages mondiaux. Les câblages français ont plutôt opté pour le câble FTP, voir ce terme.

V

V.24 : Interface de couche physique utilisée dans de nombreux pays. Très semblable à EIA-232D et RS-232-C.

Valence : Nombre d'états significatifs d'un signal. Permet pour une même rapidité de modulation d'obtenir un débit plus élevé.

Variables MIB (*Management Information Base*) : Base de données d'informations sur des objets gérés à laquelle il est possible d'accéder par des protocoles de gestion de réseau comme SNMP et CMIP.

VBR (*Variable Bit Rate*) : Classe de service dans ATM dans laquelle le débit de la source varie entre deux valeurs négociées et garanties par le réseau. Voir *ABR, CBR, UBR*.

VCI (*Virtual Circuit Identifier*) : Voir *VPI/VCI*.

VLSM (*Variable Length Subnet Mask*) : Possibilité de spécifier, pour le même numéro de réseau, un masque différent sur différents sous-réseaux. Permet d'optimiser l'espace d'adressage disponible. Est actuellement supporté par le protocole de routage OSPF et le routage statique.

VPI/VCI (*Virtual Path identifier/Virtual Channel identifier*) : Combinés, ces champs identifient une connexion au réseau ATM.

VPN (*Virtual Privat Network*) : Technique qui simule un réseau privé dans un réseau public.

VRC (*Vertical Redundancy Check*) : Contrôle vertical de redondance, technique de contrôle de parité appliquée à tous les mêmes bits d'un bloc et non à l'ensemble des bits d'un caractère (LRC, *Longitudinal Redundancy Check*).

VSAT (*Very Small Aperture Terminal*) : Système de transmission par satellite géostationnaire utilisant des antennes de faible dimension.

VT (*Virtual Terminal*, ISO 9040 et 9041) : définit un terminal virtuel (nombre de lignes, nombre de caractères par ligne, attributs de caractères, fontes...). Il assure la correspondance entre les caractéristiques du terminal virtuel et le terminal du système physique réel. VT gère les différents types de terminaux : terminal en mode défilement ou rouleau, terminal en mode page, terminal en mode masque d'écran et données, terminal graphique simple ou multifenêtre.

VTAM (*Virtual Telecommunications Access Method*) : Ensemble de programmes qui contrôle les communications entre des nœuds et des programmes d'applications tournant sur un système hôte.

W

W3 : Voir *WWW*.

W3C (*World Wide Web Consortium*) : Organisme chargé de la normalisation de HTML.

WAN (*Wide Area Network*) : Réseau recouvrant une région géographique relativement étendue. Également appelé *Réseau longue distance.* Voir aussi *LAN* et *MAN*.

Web : Voir *Word Wide Web.*

Wi-Fi : Nom commercial d'un système de transmission sans fil (IEEE 802.11).

Word Wide Web (*WWW*) : Ensemble des serveurs Web accessibles sur Internet, couramment appelé Web

WWW : Voir *World Wide Web.*

X

X.3 : Avis CCITT qui définit différents paramètres PAD.

X.500 : Avis CCITT (UIT) Service d'annuaire du monde OSI.

X-Modem : Protocole de transmission de données du domaine public.

X.21 : Avis CCITT (UIT) définissant un protocole de communication entre des unités utilisateur et un réseau à commutation de circuits.

X.25 : ou avis *X.25* du CCITT (UIT) qui définit les protocoles d'accès (protocole entre l'ETTD ou DTE et l'ETCD ou DCE) au réseau à commutation de paquets appelé réseau X.25 ou PSPDN (*Packet Switched Public Data Network*).

X.28 : Avis CCITT qui définit l'interface terminal-PAD.

X.29 : Avis CCITT qui définit l'interface ordinateur-PAD.

X.400 : Avis CCITT qui spécifie une norme de transfert électronique de fichiers.

XID (*eXchange Identification*) : Trame HDLC utilisée pour l'identification du terminal en X.25, ou pour déterminer les paramètres d'un échange dans les réseaux locaux (LLC1).

XNS (*Xerox Network System*) : Ensemble de protocoles initialement conçus par Xerox PARC.

Y

Y-Modem : Protocole de transmission de données par blocs en mode asynchrone. Ce protocole inclut un mécanisme de détection d'erreur mais pas de reprise sur erreur.

Z

Zone d'autorité : Associée au service DNS, elle correspond à une section de l'arbre de nommage sur lequel un serveur a autorité.

Z-Modem : Protocole asynchrone de transmission de données par blocs avec détection et reprise sur erreur.

© Dunod – La photocopie non autorisée est un délit

Index

Symboles

2B1Q 76
802.1Q 415

A

AAL 225, 340, 344
Abaques d'Erlang 143
Aboutement de réseaux 561
ABR 347
Accès de base 527
Accès directs 322
Accès indirects 322
Accusé de réception 206
Acheminement 171
ACK 114, 116, 119, 215
Acquittement différé 121
Acquittement global 121
ACSE 221
Adaptation d'impédance 50
Adaptative error free 412
Administration de réseau 625
ADPCM 21
Adressage 171
Adressage à plat 173
Adressage agrégé 289
Adressage de convention 176
Adressage de LS 250
Adressage géographique 249
Adressage global 173
Adressage hiérarchique 173, 287
Adressage IP 239
Adressage logique 172
Adresse 172, 243
Adresse IPv6 287
Adresse MAC 371
Adresse physique 172, 371
Adresse privée 289
Adresses privées 244
Adresses publiques 244
Adresses sur abonnement 290
ADSL 359
AFI 174
Agrégation de routes 486
Aires de routage 484
Algorithme de Dijkstra 180
Aloha 385
AMRC 542
AMRF 541
AMRT 542
Analyse spectrale 46

Anneau à jeton 395
Annuaire 177
Annulateurs d'écho 576
Annulation d'écho 83
Annuleur d'écho 51, 337
Antenne 59
Any Lan 407
Anycast 288, 290
Appels off-net 560
Appels on-net 560
Arbre de nommage 632
Architectures constructeurs 225
ARP 236, 258, 259, 379
ART 357
AS 184, 480
ASCII 15
ASN 1 219
Asymmetric data rate Digital Subscriber Line 359
Asynchrones 34
ATM 166, 186, 306, 324, 335, 448, 578
ATM Adaptation Layer 340
ATMARP 259, 450
Autorité de Régulation des Télécommunications 357
Available Bit Rate 347
Avis V.11 92
Avis V.24 93
Avis V.28 92
Avis X.21 98

B

B-ISDN 537
B00TP 261
Backbone 470
Backward Explicit Congestion Notification 330, 349
Bande de base 74, 78
Bande passante 46–48
Baud 75
BEB 388
BECN 326, 330, 349
BER 106
Best effort 168, 234, 494
BGP 185, 493
Bit 11
Bit de bourrage 72, 105, 130
Bit de parité 108
Bit de start 37
Bit de viol 72
Bit stuffing 105, 325
Bits de stop 37
Blindage 54
BLR 358
Boucle locale 158, 356
Boucle Locale Radio 358
BPSK 81
Brasseurs 304, 338
BRI 523
Bridges 467
Broadcast 173, 240, 248
Bruit 8, 77
Bus 160, 453, 455

C

Câble croisé 97
Câble droit 97
CAC 343, 348
Canal D 521, 523, 528
Canal d'écho 529
Canal de signalisation 127
Canal sémaphore 129, 323, 520, 534, 566
Canaux B 521, 523
Canaux H 521, 523
Caractère d'échappement 104, 105
CAS 128, 156, 519
CATV 54
CBDS 446
CBR 344, 346
CCBNT 525
CCBT 525
CCITT N°7 527
CCRSE 221
CCS 129, 520, 566
CDMA 542
Cell Discarding 349
Cell Loss Priority 340, 348
Cell Tagging 329, 349
CELP 22, 573
CES 578
Channel Associated Signalling 128
CHAP 274, 609
Chevaux de Troie 617
Chiffrement asymétrique 603
Chrominance 18
CIDR 249, 283
CIR 329

Circuit virtuel 168, 312
Circuit Virtuel Commuté 169, 314
Circuit Virtuel Permanent 169, 314
Class of Service 343
Classes d'adressage 241
Classes de service 25, 346
Classical IP 448, 449
Clé publique 603
Clé secrète 603
Clés asymétriques 603
Clés symétriques 602
CLLM 330
CLP 340, 348, 349
CLS 447
CMIP 627
CMIS 627
Coaxial 54
Codage 68
Codage 4B5B 73
Codage à la source 9, 68
Codage des informations 10
Codage en ligne 68
Codage Manchester 70
Codage Manchester différentiel 70
Codage NRZ 70
Code *Delay Mode* 71
Code ASCII 12
Code autocorrecteur 107
Code Baudot 12
Code bipolaire 71
Code de Huffman 14
Codec 101
Codes autocorrecteurs 113
Codes cycliques 109
Codes HDBn 72
Coefficient de vélocité 51
Commerce électronique 620
Committed Information Rate 329
Common Channel Signalling 129
Commutation 141, 185, 409, 412
Commutation de cellules 166
Commutation de circuits 163, 164, 522
Commutation de messages 164
Commutation de paquets 165, 522
Commutation de segment 412
Commutation par port 412
Commutation spatiale 164
Commutation temporelle 164
Composante continue 46, 69
Compression 20
Concentrateur 144, 145
Concentration de trafic 142
Congestion 188, 330
Connection Admission Call 343, 348
Connexion de transport 267
CONS 169
Constant Bit Rate 344, 346
Constellation de satellites 63
Contrat de service 190
Contrôle d'admission 189, 190, 328, 343
Contrôle d'erreur 105, 270
Contrôle de congestion 172, 188
Contrôle de flux 123–125, 135, 189, 205, 215, 269, 339
Contrôle de flux dynamique 125
Contrôle de flux explicite 125, 269
Contrôle de flux implicite 124
Contrôle de la congestion 269
Convergence Sublayer 340
Cordless 541
Correction d'erreur sur temporisation 114
CoS 343
Couche 196
Couche application 220
Couche homologue 196
Couche liaison de données 208
Couche physique 207
Couche présentation 218
Couche réseau 208
Couche session 217
Couche transport 212
Couches basses 201
Couches hautes 201
Couches homologues 197
CRC 109, 110, 338, 605
Crédit d'émission 119, 124
Critère de Nyquist 74, 75
CRTP 584
Cryptographie 601
CS 340
CSMA 528
CSMA/CA 420
CSMA/CD 385
CSS 568
CSTA 553
CT1 543

© Dunod – La photocopie non autorisée est un délit

CTI 553
Cut through 412
CVC 312, 314
CVP 314

D

Datagramme 168
Datagramme IP 252
DBR 346
DCE 42
DCS 539
DCS1800 543
Débit binaire 8
Débit de cadrage 150
Débit effectif 39
Débit nominal 39
Débit réel 39
Délai de paquetisation 192
Delay skew 51
DES 603
Désadaptation d'impédance 50
Détection d'erreur 107
Détection par écho 107
Détection par répétition 107
Deterministe Bit Rate 346
DHCP 261, 262
Dial-up 307
Dialogue de bout en bout 199
Dialogue en mode point à point 199
Diaphonie 52
Diffie-Hellman 605
DiffServ 253, 356, 495, 496
Diffusion dirigée 243
Diffusion générale 243
Diffusion limitée 243
Diffusion réduite 243
Diffusion restreinte 243
Discard Eligibility 329
Distance de Hamming 113
Distorsion 47
DLCI 326, 327
DMT 359
DMZ 615
DNIC 174
DNS 235, 275, 276, 589, 614
Domaine de nommage 275
Données analogiques 9
Données continues 9
Données discrètes 9
Données isochrones 25
DPAM 407
DPNSS 568
DQDB 440
DSA 229
DSI 572
DSL 359
DSP 174
DTE 41
DTMF 518, 553
DTP 222

E

E.163 517
E.164 517
E1 152, 564, 565
Échantillon 16
Écho 50
Éclatement des connexions 205
EFCI 349
EFCN 349
Efficacité 118
Efficacité du protocole 117
EGP 184, 185, 480, 493
EIR 329
ELAN 453
Éliminateur de modem 97
E&M 562
Émulation de terminal 369
Encapsulation de données 197
Enregistreur 515
Entropie 13
Erlang 557
ETCD 42
Ethernet 385, 390–392, 413, 431, 452
Ethertype 237, 384, 389, 417
Étiquette 151
ETR 432
ETTD 41
EUI-64 288
Excess Information Rate 329
Explicit Forward Congestion Indication 349
Explicit Forward Congestion Notification 349
External Gateway Protocol 184

F

F/TDMA 542
Faisceaux de lignes 558
Faisceaux hertziens 60
Fanion 104, 129
Fast Ethernet 392
Fast forward 412
FCS 110, 130, 310, 328, 427
FDB 409
FDDI 431
FDDI-II 439
FDMA 541
FECN 326, 330
Fenêtre d'anticipation 119
Fenêtre de collision 387
Fenêtre de réception 122
Fenêtre dynamique 269
Fenêtre glissante 120
Fenêtre stupide 269
Fext 52
Fiabilité 599
Fibre Channel 426
Fibre monomode 57
Fibre multimode 57
Fibre optique 55, 58
Fibres à gradient d'indice 57
Fibres à saut d'indice 57
Filtre 48
Firewall 614
Flag 129
Fondamental 9, 46
Forward Explicit Congestion Notification 330
Fourier 9, 46
FR11 335
FRAD 326, 331
Fragmentation 255, 287
Fragments 187
Frame 129
Frame Check Sequence 130
Frame Relay 186, 306, 324
Fréquence de coupure 48
FTAM 222
FTP 52, 235, 280
Full duplex 30, 83
FXO 578
FXS 578

G

G.711 22
G.729 22
G.729a 573
Gel de référence 214
Gigabit Ethernet 394
Gigue 9, 297, 298, 344, 496, 575
Glissement 298
Globalstar 547
Go Back N 122
GPRS 544
GPS 299
GSM 538, 539, 543

H

H.225 585
H.245 585
H.323 585
Half duplex 29
Hand over 538, 541
Harmoniques 9, 46
Hayes 85
HDLC 129, 133
HEC 338, 339
Hello 487
Hiérarchie plésiochrone 298, 300
Hiérarchie synchrone 298, 302
HiPPI 32, 426
Horloge 34, 35
Host_ID 241, 242, 245, 288
HTTP 235
Hub 391, 392

I

I-Mode 546
IAB 238
IANA 238
ICI 199
ICMP 235, 254, 256, 257, 611
IDI 174
IDU 199
IETF 238
IFG 389
IGMP 500
IGP 184, 480, 493
IGRP 185, 483
ILMI 454

© Dunod – La photocopie non autorisée est un délit

Impédance caractéristique 49
Intensité de trafic 142, 143
Interface non numérotée 251
Interior Gateway Protocol 184
Intervalle de temps 149
IntServ 495
IP 234, 236
IP Precedence 253, 494
IPSec 605, 610
IPv6 283
IPX/SPX 422
Iridium 546
IS-IS 185
ISN 264
ISO 195
Isochrone 191
ISP 89
IT 149, 512
Itinérance 538, 542

J

Jam interval 388
Jeton 373, 378, 396, 404, 439
Jitter 9, 297
Jonction 42, 90
JTM 223

L

L2F 619
L2TP 619
Label 151, 186, 356
LAN 158, 368
LAN ATM 259, 448
LAN Emulation 449, 452
LAN Emulation Configuration Server 453
LAP-B 133, 309
LAP-D 527, 531
Large bande 78
Largeur de bande 9, 47, 48
LASER 56
LCP 274
LDAP 590
LECS 453
LEO 546
LES 453
LIA 562
LIA à changement d'état 563
LIA à courant continu 563
LIA à impulsions codées 563
LIA à impulsions codées 50 Hz 563
Liaison point à point 160
Liaison virtuelle 327
Liaisons hertziennes 59
Link status 392
LIS 259, 449
Lissage de trafic 189, 190
LLC 370, 381–383, 397
LMI 330
Local Area Network 158, 368
Logical Link Control 370
Loi μ 17
Loi A 17, 21
Loopback 242
LRC 108
LU 227
Luminance 18

M

MAC 173, 236, 258, 370, 377, 397, 409, 467
Mainframe 30
Maintenabilité 599
MAN 158, 431, 440
Management Information Base 353
Manchester 389
Manchester différentiel 399
MAQ 82
Masque de sous-réseau 246
Medium Access Control 173, 370
Metropolitan Area Network 158
MGCP 591
MHS 222
MIB 353, 626, 628, 630, 631
MIC 562, 572
Minitel 145
Mixtes 558
MNP 84
Mode connecté 168
Mode datagramme 168
Mode dissymétrique 40
Mode non connecté 168
Mode orienté connexion 168, 169
Mode symétrique 40
Modèle de référence 196, 202
Modèle OSI 195
Modem 78, 87
Modulation 79

Modulation d'amplitude 79
Modulation de fréquence 79, 81
Modulation de phase 79, 81
Modulation en amplitude à porteuse en quadrature 82
MPLS 186, 356
MPOA 458, 459
MSS 238
MTBF 599
MTTR 599
MTU 187, 238, 401
Multicast 173, 242, 288, 290, 336
Multiplex 149, 150, 299, 300
Multiplexage 146
Multiplexage d'étiquette 151
Multiplexage de longueur d'onde 148
Multiplexage de position 151
Multiplexage des connexions 205
Multiplexage fréquentiel 147
Multiplexage par étiquette 165, 337
Multiplexage spatial 147
Multiplexage temporel 149
Multiplexeur 144, 146, 304, 570
MultiProtocol Label Switching 356
Multisite 567

N

NAT 244, 283, 613
NBMA 485, 488
NCP 274
Net_ID 241, 242, 245, 283
NetBEUI 425
NetBIOS 424
Network Operating System 370
Next 52
NIC 378
NNI 339
Node 30
Nommage 171, 176
NOS 370
NRZ 69
NSAP 174, 209
NUA 174
Null modem 97
Numérisation 9, 15
Numéro de séquence initial 264
Nyquist 16

O

ODA 222
Off-net 561
On-line 307
On-net 561
Onduleur 598
Option 255
Organization Unit Identifier 378
OSFP 236
OSPF 185, 484
OUI 378, 384

P

PABX 523, 549, 550, 557, 560
PABX de transit 574, 578
PAD 145, 313, 320, 321
Paging 537
Paire torsadée 51
PAP 274, 609
Paquet 165
Paquetisation de la voix 192
Parabole 60
Paradiaphonie 52
Pare-feu 614
Passerelle 145
PAVI 145
PCI 199
PDH 153, 296, 300, 512
Piggybacking 133, 268
PIN 539
PING 257
PKI 607
Plesiochronous Digital Hierarchy 153
PNNI 351
Point d'accès au service 197
Point of Presence 355
Point to Point Protocol 137
Poison reverse 482
Polynôme générateur 109–112
Pont racine 471
Ponts 467
Ponts à routage par la source 468, 474
Ponts transparents 468, 469
PoP 355
Port 237, 265
Porteuse 78
POTS 360

© Dunod – La photocopie non autorisée est un délit

PPP 137, 236, 272, 273
PPTP 619
Précâblage 53, 375
PRI 523
Primitives 210
Primitives de service 197
Private Network to Network Interface 351
Probabilité de refus 558
Protocole 103, 196, 237
Protocole D 527, 533, 566
Protocole d'accès 368
Protocole de niveau N 197
Protocole de routage 178
Protocole orienté bit 130
Protocole PPP 609
Protocoles asynchrones 37
Proxy-Server 617
Pseudo en-tête 270
PU 226
PVC 450

Q

Q-SIG 568
Q.23 518
Q.931 585
QAM 82
QoS 343, 494
Qualité de service 24, 206, 494
Quantité d'information 11

R

RAID 596
Rapidité de modulation 74, 75
Rapport signal sur bruit 8, 77
RARP 236, 242, 259
RAS 617
RDA 223
Réassemblage 187
Référence d'appel 531
Référence de transport 214, 265
Rejet sélectif 122
Rejet simple 122, 135
Relais 199
Relation de Shannon 77
Répéteurs 298
Reprise sur erreur 107, 119, 122, 135
Réseau 157
Réseau à commutation 158, 162
Réseau à diffusion 160
Réseau de diffusion 158
Réseau maillé 161
Réseau plésiochrone 159
Réseau synchrone 159
Réseau virtuel 158
Réseaux 144
Réseaux « ad hoc » 418
Réseaux arborescents 161
Réseaux cellulaires 419
Réseaux sans fil 417
Réseaux voix/données 570
Résolution de nom 276
Resolver 276
Retransmission Time Out 114, 134
Return Loss 51
RIP 185, 235, 422, 481
RIPE 239
RMON MIB 630
RNIS 549
RNIS large bande 537
Roaming 538, 542
RON/TRON 562
ROSE 222
Round Trip Time 116
Routage 171, 185
Routage à état des liens 180, 484
Routage à plat 184
Routage adaptatif 169
Routage au moindre coût 179
Routage de Bellman-Ford 179
Routage fixe 178
Routage hiérarchique 184
Routage interdomaine 493
Routage multicast 498
Routage par diffusion 178
Routage par inondation 178
Routage par la source 352, 400
Routage par le chemin le plus court 179, 480
Routage statique 178
Routage statique ou fixe 480
Routage vecteur distance 179, 481
Routeur 477, 479
RPIS 560
RS232C 93
RSA 604
RSVP 495, 582

RTC 511, 549
RTO 114, 134
RTP 582
RTSE 221
RTT 116

S

S-HTTP 609
SABM 133
SAP 198
SAPI 527, 528, 531
SAR 340
Satellite 61
SBR 346
SDA 526, 560
SDH 153, 296, 299, 302, 303, 305
Segmentation 172, 187
Segmentation and Reassemblage 340
Sélection Directe à l'Arrivée 526
Send and Wait 114
Services supports 524
Shannon 16
Signalisation 126
Signalisation canal associé 156
Signalisation CAS 564
Signalisation dans la bande 127, 302
Signalisation hors bande 127
Signalisation par canal sémaphore 562
Signalisation par vol de bits 127
Signalisation voie par voie 128, 156, 302, 562
Signature numérique 607
Silly Window Syndrome 269
SIM 539
SIP 588
Site Level Aggregator 289
Site local 289
SLA 289, 496
SLIP 236, 272, 273
SMAE 627
SMAP 627
SMDS 446
SMS 539
SMTP 235
SNA 226
SNAP 384, 502
SNMP 235, 353, 630, 634
SNPA 209
Socket 234, 265, 424
SONET 303
Source Routing 438, 474
SPA 558, 559
Spanning tree 471
Spanning Tree Protocol 401, 471
SPB 558, 559
Spectre de fréquences 47
Spectre du signal 9, 46, 47
Split horizon 481
Splitter 360
SS7 350, 534, 536, 566
SSCP 226
SSL 610
Statistical Bit Rate 346
STM 151
Store and forward 412
STP 52
SubNet_ID 245
Supernetting 249
Supports de transmission 45
Surdébit 150
Surdébit de cadrage 150
Sûreté 595
SVC 312, 450
Synchrones 34
Synchronisation 34
Synchronisation caractère 104
Synchronous Digital Hierarchy 153
Synchronous Transfer Mode 151
Syntaxe abstraite 218
Syntaxe concrète 218
Systèmes autonomes 184

T

T.120 585
T0 523
T1 523, 564, 565
T2 523
Tables d'acheminement 177
Tables de routage 177
Taille de la fenêtre 119
Taux d'activité 142, 149
Taux d'erreur 8
Taux d'erreur binaire 105, 106
Taux de compression 20
TCP 263

© Dunod – La photocopie non autorisée est un délit

TCP/IP 233
TDMA 542
TEI 527, 528, 531
Télédiaphonie 52
Téléservices 524, 550
Telnet 235, 281
Temporisateur 114
Temps de retournement 97
Temps réel 191, 223
Terminal virtuel 281
Terre de protection 67
Terre de signalisation 40, 67, 92
TFTP 235, 278
Three ways handshake 215
THT 433
Tiers de confiance 607
Time Out 114
Time slot 387
TNA 523
TNL 522
TNR 522, 528
ToIP 581
Token 373, 378
Token Bus 403
Token Ring 396, 452
Tolérance de panne 595
Topologie 372
Topologie étoile 160
Topologie en anneau 160
Topologie logique 159
Topologie physique 53, 159
Trame MIC 152
Trames d'information 129
Trames de supervision 129
Trames non numérotées 129
Tranche canal 387
Translation d'adresses 245, 613
Transmission asynchrone 34, 36
Transmission bande de base 78
Transmission différentielle 40
Transmission en bande de base 68
Transmission large bande 68, 78
Transmission parallèle 32
Transmission série 33
Transmission synchrone 34, 38
Transparence 104
TRT 433
TTRT 433, 439
Tunnel 465
Tunnel de niveau N 197
Type de service 253

U

UBR 347
UDP 234, 271
UMTS 545, 546
UNI 339
Unicast 173, 288, 336
Unicode 15
Unspeciefied Bit Rate 347
URAD 515, 561
UTP 52, 407

V

V.24 99
V.42 84
V.42bis 84
V.90 89
Valence 77
Valence du signal 75
Variable Bit Rate 345, 346
VBR 345, 346
VBR Real Time 346
VBR-nrt 347
VBR-rt 346
VCC 336
VCI 337
VFRAD 579
Virtual Area Network 413
Virtual Channel Connection 336
Virtual Channel Identifier 337
Virtual Path Identifier 337
Virus 617
VLAN 413, 414
VoFR 579
Voie composite 146
Voie incidente 146
Voie par voie 519
Voie temporelle 149
Voies virtuelles 128
VoIP 581
Voix paquetisée 571
Voix/données 191
VPI 337
VPID 416

VPN 617
VRC 108
VT 222
VTOA 579

W

WAN 158
WAP 545
WDM 148, 306, 354
Wide Area Network 158
Wireless Local Loop 358
WLAN 417
WLL 358
WMAN 417
WPAN 417
WWAN 417

X

X.121 174, 313
X.21 bis 99
X.25 307
X.500 222
XNS 422
XON, XOFF 124

© Dunod – La photocopie non autorisée est un délit